Aphelion 3300AG
802.11a/b/g Dynamic Expansion Outdoor Wireless Access Point

User Manual

V.06.6.19

June, 2006

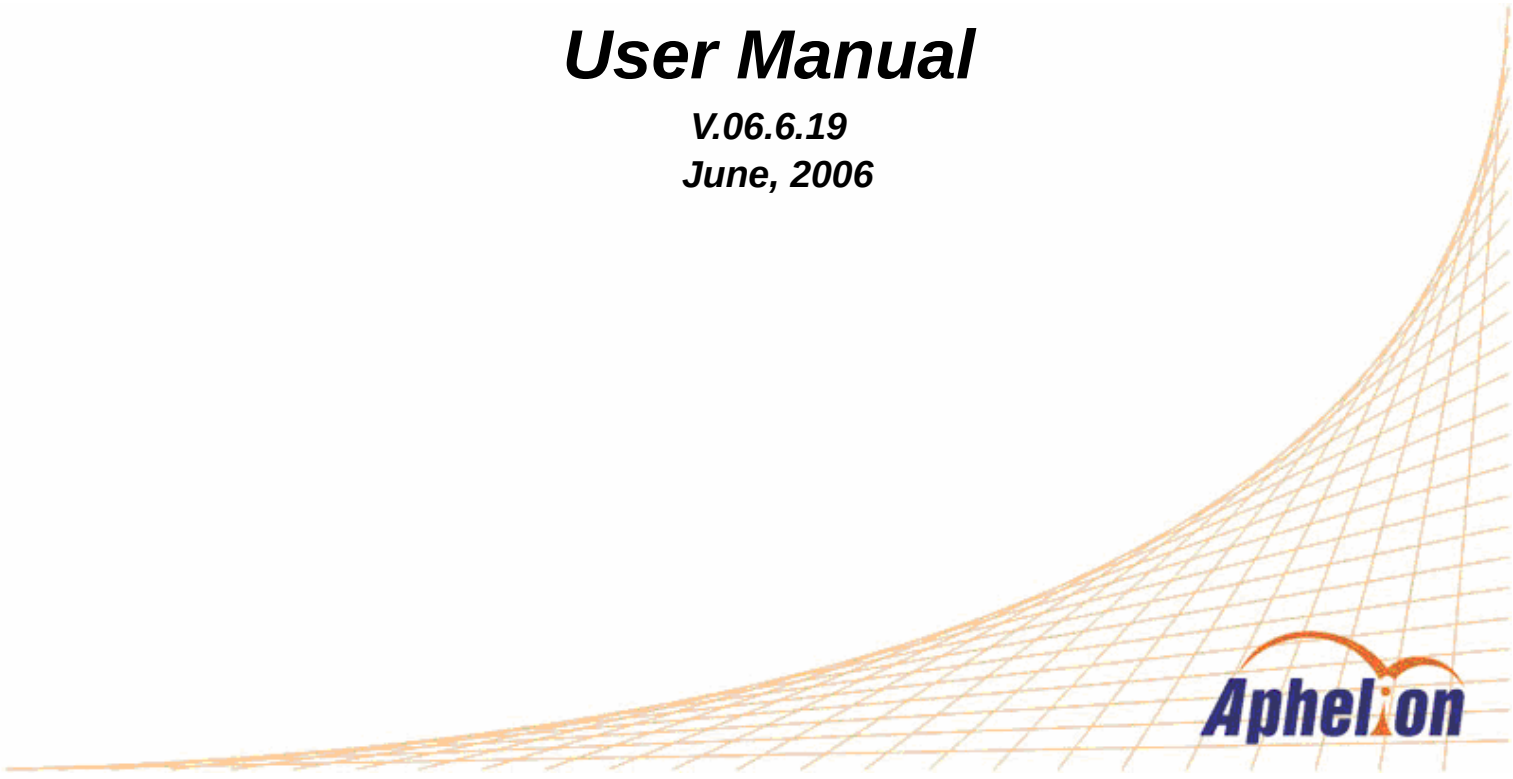


Table of Contents

Chapter 1. Warranty and Support 1

1.1. Warranty 1

1.2. Technical Support 5

Chapter 2. Aphelion 3300AG 6

2.1. Features 6

2.2. Specifications 7

Chapter 3. Hardware Installation 11

3.1. Package Contents 11

3.2. Hardware Description 12

3.3. Outdoor Installation 16

Chapter 4. Basic Configurations 20

4.1. Aphelion System Menu Tree (SMT) 20

4.2. General Configuration 20

4.3. Advanced Setting 25

4.4. System Management 35

4.5. System Monitoring 39

Chapter 5. Application Notes 46

5.1. Point to Point Installation 46

5.2. Hard Reset to Factory Default 52

5.3. Firmware Upgrade 53

Appendix 58

I. Antenna concepts and Installations 58

II. Wireless Security Concept 60

III. Glossary 64

Chapter 1. Warranty and Support

This chapter describes Aphelion's warranty policy and support

1.1. Warranty

Subject to the terms and conditions set forth herein, Aphelion Communications Inc, Aphelion provides this Limited Warranty:

Only to the person or entity that originally purchased the product from Aphelion or its authorized reseller or distributor.

Limited Warranty: Aphelion warrants the hardware portion of the Aphelion product as follow: Hardware will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (Warranty Period) except as otherwise stated herein.

Hardware (excluding power supplies and fans): One (1) Year
Power supplies and fans: One (1) Year
Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of Aphelion and its suppliers under this Limited Warranty will be, at Aphelion's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by Aphelion at an authorized Aphelion Service Office. The replacement hardware need not be new or have an identical make, model or parts. Aphelion may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that Aphelion reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if Aphelion determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by Aphelion upon return to Aphelion of the defective Hardware. All Hardware or parts thereof that are replaced by Aphelion, or for which the purchase price is refunded, shall become the property of Aphelion upon replacement or refund.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for

Hardware and Software portions of Aphelion's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which Aphelion, the distributors, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "as-is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to Aphelion as outlined below:

The customer must submit with the product as part of the claim a written description of the Hardware defect or Software non-conformance in sufficient detail to allow Aphelion to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

Aphelion Technical Support Team will attempt to assist the customer in resolving any suspected defects with the product, and can be contact at support@aphelions.com. If the product is considered defective, the customer must obtain a Return Material Authorization (RMA) number by contacting sales@aphelions.com.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. Aphelion will only replace the defective portion of the product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to Aphelion. No Cash on Delivery (COD) is allowed. Products sent COD will either be rejected by Aphelion or become the property of Aphelion. Products shall be fully insured by the customer and ship back to Taiwan. Aphelion will not be held responsible for any packages that are lost in transit to Aphelion. The repaired or replaced packages will be shipped to the customer via DHL Ground or any common

carrier selected by Aphelion. Return shipping charges, we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

Aphelion may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay Aphelion reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by Aphelion not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by Aphelion does not cover: Products that, in Aphelion judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than Aphelion; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which Aphelion, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an authorized Aphelion Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: Except for the Limited Warranty specified herein, the product is provided without any warranty of any kind whatsoever including, without limitation, any warranty of merchantability, fitness for a particular purpose and non-infringement. If any implied warranty cannot be disclaimed in any territory where a product is sold, the duration of such implied warranty shall be limited to the duration of the applicable warranty period set forth above. Except as expressly covered under the limited warranty provided herein, the entire risk as to the quality, selection and performance of the product is with the purchaser of the product.

Limitation of Liability: To the maximum extent permitted by law, Aphelion is not liable under any contract, negligence, strict liability or other legal or equitable theory for any loss of use of the product, inconvenience or damages of any character, whether direct, special, incidental or consequential (including, but not limited to, damages for loss of goodwill, loss of revenue or profit, work stoppage, computer failure or malfunction, failure of other equipment or computer programs to which Aphelion product is connected with, loss of information or data contained in, stored on, or integrated with any product returned to Aphelion for warranty service) resulting from the use of the product, relating to warranty service, or arising out of any breach of this Limited Warranty, even if Aphelion has been advised of the possibility of such damages. The sole remedy for a breach of the foregoing Limited Warranty is repair, replacement or refund of the defective or non-conforming product. The maximum liability of Aphelion under this warranty is limited to the purchase price of the product covered by the warranty. The foregoing express written warranties and remedies are exclusive and are in lieu of any other warranties or remedies, express, implied or statutory.

Governing Law: This Limited Warranty shall be governed by the laws of the Taiwan. Some countries do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: Aphelion is a registered trademark of Aphelion Communications Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Aphelion Corporation/Aphelion Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2004 by Aphelion Corporation/Aphelion Systems, Inc. All rights reserved.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local Aphelion office.

1.2. Technical Support

Aphelion believes in ONE goal as to achieve total customer satisfaction; for any technical assistance or information assists, please go to the support section of our website www.aphelions.com, email to support@ aphelions.com or where we have professional engineers standing by to assist you.

If you are a qualified distributor of Aphelion, you will be getting usernames and passwords for supporting online where you will find many useful application notes and FAQs.

Please have the following information ready when you contact Aphelion support:

- Serial number and model name.
- Firmware version in system monitoring menu.
- Application of which you are deploying with Aphelion 3300AG and network topology.

Thank you

Chapter 2. Aphelion 3300AG

This chapter describes Aphelion 3300AG in brief for your applications

2.1. Features

Aphelion 3300AG is a carrier class outdoor wireless access point which offers a robust and high quality performance solution for point-to-point, point-to-multi points and HotZone applications in both license free 2.4GHz and 5GHz bands. Superior performance is the key feature in Aphelion 3300AG. With three radios, 3300AG could sustain high performance and extending coverage. The Aphelion 3300AG is the most ideal candidate for service providers looking to deliver carrier class wireless services to multiple market segments such as campuses, hospitality, and wider metropolitan area deployments.

- Features in a Glance :
  Dynamic expansion daisy chain wireless Hot Zone
  Low latency and high throughput upon multiple wireless hops
  Scalable wireless distribution platform
  Reliable performance when deploying multiple nodes in bridged or routed environments.
  Bandwidth control module at subscriber level

- Comprehensive Security Features :
  802.1x EAP support (client and server modes)
  EAP-MD5, EAP-TLS support and Dynamic WEP Keys
  RADIUS client
  Hide ESSID
  MAC address filtering
  NAT
  SSH secure telnet

- Dynamic WAN Interface Assignments :
  Easy assignments of WAN to fit in different network topology
  Flexible wireless network distribution system

- Harsh Outdoor Environments Sustainable
  Sturdy water-tight housing
  Built-in heater module to facilitate cold regions
  PoE module

- System Management :
  Firmware upgrade through TFTP, FTP
  Interface status display
  SNMP v1/v2

- Simple Installation and Deployment :
  Software Alignment / Deployment Tools

2.2. Specifications

Standard support	Wireless	IEEE802.11a IEEE802.11b/g
	Ethernet	IEEE802.3 IEEE802.3u IEEE802.3af (Power over Ethernet (PoE), 48VDC 1A, Standard IEEE 802.3af cabling. Max consumption 26 W)
Interface	Consol	RS 232 Port
	Ethernet	1×10/100 Base-T RJ-45 Power over Ethernet(PoE)
	Wireless	Antenna Connector: 3 ㄨ Reversed Female N-type
Memory	SDRAM	64Mbyte
	Flash	32Mbyte
Ethernet	Max. Bandwidth	Full Duplex: 100Mbps (100Base), 10Mbps (10Base)
System Setting	Operation Mode	AP / AP Client / Bridge / Router
	RF Interface Application	Support Dynamic WAN Interface assignments
	Frequency Range	**USA:** 2.400 – 2.483GHz, 5.15 ~ 5.35Ghz, 5.725 ~ 5.825Ghz **Europe:** 2.400 – 2.483GHz, 5.15~ 5.35Ghz, 5.47 ~ 5.725Ghz **Japan:** 2.400 – 2.483GHz, 4.90 – 5.091GHz, 5.15 – 5.25GHz **China:** 2.400 – 2.483GHz, 5.725 ~5.85Ghz
	Modulation Technique	**802.11b/g** DSSS (DBPSK, DQPSK, CCK) OFDM (BPSK,QPSK, 16-QAM, 64-QAM) **802.11a** OFDM(BPSK,QPSK, 16-QAM, 64-QAM)

	Channels Support	**802.11b/g** US/Canada: 11 (1 ~ 11) Major European country: 13 (1 ~ 13) France: 4 (10 ~ 13) Japan: 11b: 14 (1~13 or 14th), 11g: 13 (1 ~ 13) China: 13 (1 ~ 13) **802.11a** 1). US/Canada:12 non-overlapping channels (5.15 ~ 5.35GHz, 5.725 ~ 5.825GHz) 2). Europe: 19 non-overlapping channel (5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz) 3). Japan: 4 non-overlapping channels (5.15 ~ 5.25GHz) 4). China : 5 non-overlapping channels (5.725 ~ 5.85GHz)
	Transmitted power	802.11b mode: 18dBm 802.11g mode: 18dBm @ 6Mbps 15dBm @ 54Mbps 802.11a mode: 17dBm @ 6Mbps 13dBm @ 54Mbps
	Receiver Sensitivity	Receiver sensitivity: (PER < 8% for 11b ; PER < 10% for 11g &11a) 802.11b Sensitivity: DBPSK (1Mbps) -93dBm DQPSK (2.2Mbps) -92dBm CCK (5.5Mbps) -90dBm CCK (11Mbps) -88dBm 802.11g Sensitivity: BPSK(6Mbps) -89 dBm BPSK(9Mbps) -88 dBm QPSK(12Mbps) -86 dBm QPSK(18Mbps) -85 dBm 16QAM(24Mbps) -83 dBm 16QAM(36Mbps) -80 dBm 64QAM(48Mbps) -77 dBm 64QAM(54Mbps) -72 dBm 802.11a Sensitivity: BPSK(6Mbps) -88 dBm BPSK(9Mbps) -87 dBm QPSK(12Mbps) -85 dBm QPSK(18Mbps) -84 dBm 16QAM(24Mbps) -82 dBm 16QAM(36Mbps) -80 dBm 64QAM(48Mbps) -76 dBm 64QAM(54Mbps) -71 dBm
	Wireless Transmission Rate	802.11b/g: 11, 5.5, 2, 1 Mbps, auto-fallback, up to 54 Mbps 802.11a : 54, 48, 36, 24, 18, 12, 9, 6Mbps, auto-fallback
	Wireless Other Setting	IEEE 802.11a/b/g Mode Selection Enable / Hide ESSID 802.1q VLAN-Multi SSID MAC Address Filtering Bandwidth Control of Wireless Client

		DHCP Client / Server, Fixed IP NAT Static Routing SNMP v1&v2 RIP v1&v2 Dual Image (back up) Trunk: Trunking, Smart Traffic Load Balance, One Way Transmit, Failover Roaming (Under Aphelion wireless daisy chain deployment will be required) MS NetBIOS IP Filter Enable / Disable 802.11h - Dynamic Frequency Selection (DFS) & Automatic Transmit Power Control (Auto TPC) 802.11e WiFi QoS (ready on Q3,2006) Wireless Station Fix AP MAC Address Optional Software Alignment / Deployment Tools
Wireless Security	SSID	Support Enable / Disable Broadcast Support Multi-ESSID
	WEP	Support 64bit / 128bit / 152bit Data Encryption Authentication type: Open System / Shared Key
	802.1x	Support 802.1x Client and Server
	Radius	Support Radius Client
	WPA	WI-FI Protected Access (EAP, TKIP)
	WPA2	AES / 802.11i
	MAC	Support MAC Address Filtering
	Firewall	Support NAT (net filter)
Configuration & Management	Software / Firmware	SMT management menu access via console, telnet and secure SSH telnet to implement including: System configuration & management、Firmware upgrade、Reset to default and configuration backup …etc.
Physical Spec.	Power	DC 48Volt / 1A ; AC Adapter 100V~240V Support Power over Ethernet (PoE) Power Consumption: 13W
	Dimension	L × W × H: 226 × 197 × 79 mm
	Weight	1800g
	Dusty/Waterproof	IP68 Certified
	Antenna	Reversed N-type (Option)
Regulation and	US	FCC Part 15 Class B & C & E

Compliance	Europe	ETS 300 328, ETS 301 489-1&17, ETS 301 893 ,EN 60950 compliant and CE Mark
Environment Spec.	Operating Temp	Non Heater：-30~65 ℃ With Heater：-40~65 ℃ Built-in heater module is option.
	Storage	-40℃ ~ 80℃
	Humidity	0% ~ 95% non-condensing

Notes on 802.11a operation frequency:

Some countries has allocated certain 802.11a frequency bands strictly for indoor use only, for example :

CE : 5.15 ~ 5.35GHz is for indoor only. Outdoor should use 5.47 ~ 5.725GHz.

FCC : 5.15 ~ 5.25GHz is for indoor only.

DGT : 5.15 ~ 5.25GHz is not allowed to use. 5.25 ~ 5.35GHz is for indoor only.

Japan : 5.15 ~ 5.35GHz for indoor only. Need to change the band to 4.9GHz.

Do make sure the operation frequency of 3300AG follows your local regulation. Some areas may have penalty when operating outdoor AP in a wrong frequency band. Aphelion Communications Inc. takes no responsibility for any penalty or loss caused by using illegal frequency band for Aphelion 3300AG.

Chapter 3. Hardware Installation

This chapter describes the installation procedure of Aphelion 3300AG

3.1. Package Contents

1

2

3

4

5

6

7

8

9

10

1. Aphelion 3300AG 802.11a/b/g Outdoor Wireless Access Point
2. PoE Power Injector
3. AC Power Cord
4. 2m MIL-C-5015 IP67 RS-232 Console Cable
5. 30m MIL-C-5015 IP67 Cat-5 Ethernet Cable
6. Wall Mounting Kit & Screw
7. Mast Mounting Kit & Screw
8. Grounding Wire
9. Quick Installation Guide
10. CD: User Manual

Please contact your local distributor if any of the above items is missing.

3.2. Hardware Description

1. The Outdoor AP Unit

The outdoor AP unit has three antenna ports on top, one data/power port and one console port at the bottom. The antenna ports are N-type female connectors. The data/power port is used to link to the cable from the PoE. When the outdoor AP unit and the PoE are connected together with proper power supply, the outdoor unit is turned on and initialized. The console port is used at the initial setup and to connect to the antenna alignment kit.

Front view of Aphelion 3300AG

Case Spec.

1. L × W × H: 226 × 197 × 79 mm
2. L × W × H: 245 × 197 × 79 mm (including connectors)
3. Weight: 1800g
4. Material: aluminums alloy

Top view of RF antenna connectors of 3300AG

RF antenna connectors are major interfaces on the top side of Aphelion 3300AG. It is a female N-type RF antenna connector with special waterproof.

Bottom view of power/signal connector port & console port of 3300AG

The port on right side of the photo is power/signal connector port. It is an 8-pin female connector with MIL-C-5015 IP67 waterproof. Connecting to the Power & Data Output Port of PoE.

The port on right side of the photo is Console port (TBD). It is an 8-pin male connector with MIL-C-5015 IP67 waterproof. Connecting to the PC for initial configuration and diagnostics & troubleshooting.

2. PoE Power Injector

PoE Power Injector is used to combine the data stream and power into one cable. It has three ports, AC IN is for 100~240V AC power from AC Power Cord, Data Input Port is connected the customer premises equipment (CPE) by Cat-5 cable, and Power & Data Output Port is connected to the outdoor unit by the cable described in item 5.

Connections

Antenna Connector: 3 ㄨ Reversed Female N-type
Connect to Antenna base by **Male to Male N-type** CFD 400 RF Cable

Special Consol Port
Connect one end of the 2M MIL-C-5015 IP67 RS-232 console port cable to this port; connect the other end to a Serial Port on a computer that is running a terminal emulation program; connect the another end to a Serial Port on a notebook or PDA that is running Alignment / Deployment tools program for technicians to analysis RF equipments.
Note: Use this console connection only if you are configuring the Aphelion 500AG via the console.

Special Ethernet Port
Connect one end of the 30M MIL-C-5015 IP67 Cat-5 Ethernet Cable into this port; connect the other end into the Power and Data Output Port on Inline Power Injector.

Power & Data Output Port
Attach one end of the IP67 Cat-5 Ethernet cable to this port;
attach the other end to the 30M IP67 Cat-5 Ethernet Port on the Aphelion 500AG.

Data Input Port
Connect one end of the cross-over Ethernet cable to this port; connect the other end to the Ethernet port on the computer.

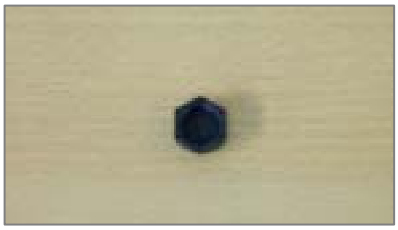
3. AC Power Cord

The AC Power Cord is to supply the 100~240V power for PoE Power Injector.

4. Cat-5 Ethernet cable with MIL-C-5015 connector

The Cat-5 Ethernet cable with MIL-C-5015 IP67 is used to provide the path to deliver power for the outdoor unit and the data communication.

5. RS-232 console cable (2m MIL-C-5015 IP67 RS-232 Console Cable) RS-232 cable is used to connect the console port of the outdoor unit and the antenna alignment tools or the workstation. One (RS-232) console port has **black color** for setting up initial configuration information, and another (RS-232) console port **(blue color)** for antenna alignment /deployment tools. The appearance of the RS-232 cable is shown below.



Water proof hat

6. Mounting Kit

The mounting kit is used to provide a good support for the outdoor unit and the

flat panel antenna. Please follow the installation procedure to mount the outdoor unit and the flat panel antenna. The contents of the mounting kit are shown below.

A. Wall Mounting Kit

B. Mast Mounting Kit

7. Grounding wire

The grounding wire is used to provide the grounding path for the outdoor unit to minimize the impact of lightening and surge.

3.3. Outdoor Installation

Aphelion 600AG can be mounted on walls or on an antenna mast as shown in the following：

Step 1 Compose the holder of Aphelion 600AG

Step 2 Connect the female end of the power cord into the PoE Injector, and connect the male end of the power cord into a power outlet. The red Power LED at the front of the PoE Injector will be on.

Step 3 Connect RJ-45 Ethernet connector from Aphelion 600AG into the Power & Data Output port on the PoE Injector. When Aphelion 600AG receives power over the Ethernet cable, Aphelion 600AG will start its boot sequence and the yellow Active LED at the front of the PoE will be on.

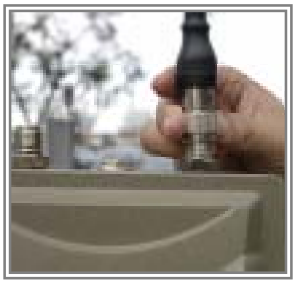
Step 4 Run the Ethernet cable from Data Input Port（on the front of the PoE Power Injector）to the Ethernet Port on the PC or notebook.

Step 5 Connect MIL-C-5015 RJ-45 Ethernet cable into MIL-C-5015 Ethernet port on the back of the access point.

Step 6: Connect RS-232 Cable（Console Port cable） to serial port. Connect the other end of RS-232 （the black one or the one marked with a black dot） to a serial port on a PC for setting up initial configuration; the other connector at the same end of RS-232（the blue one or the one without a black dot）is for antenna alignment /deployment tools.

NOTE: This connection is required for setting initial configuration. After configuration is completed, this cable may be removed and put the waterproof hat on until additional configuration is required via serial port.

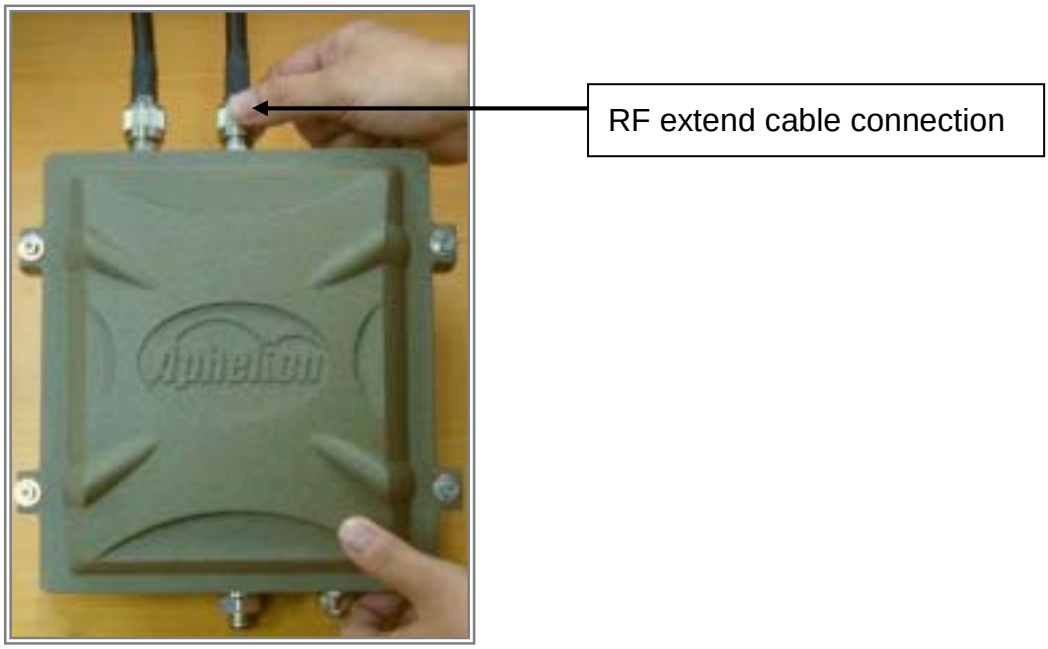
Step 7 Connect the antenna to the antenna connector shown as follow.



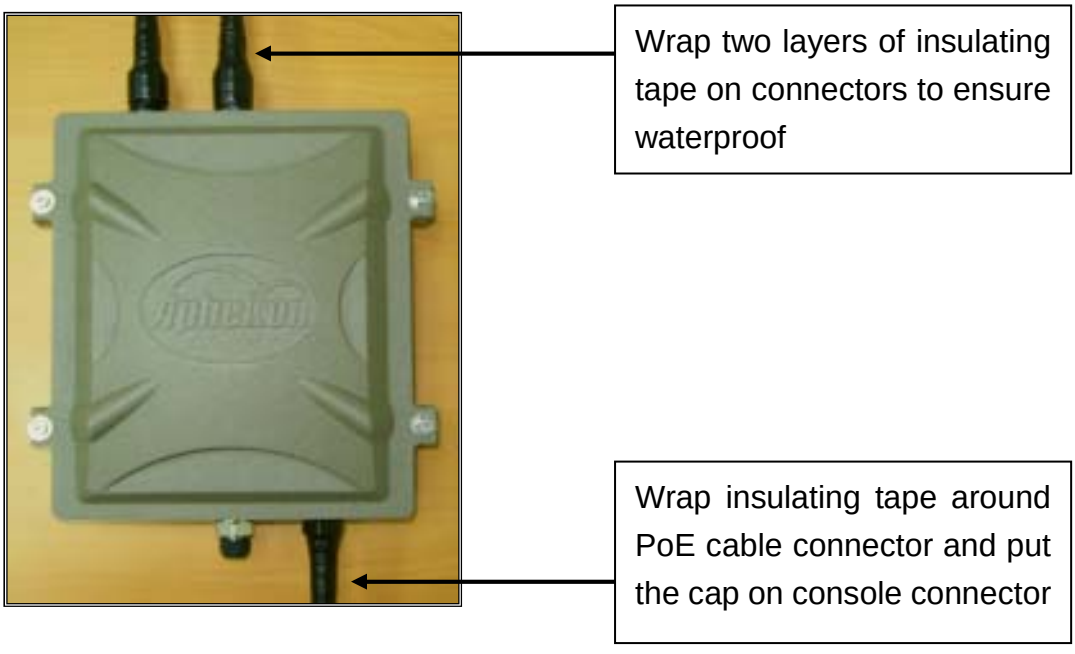
Special Notice for Waterproof Installation

Most of the problems for outdoor models are from the connector connections that loosen over time due to vibration or other forces, even allowing moisture to penetrate the connector and seriously affecting the data and radio signal transmit. The following recommendation is used for all outdoor installation to be waterproofed.

Step1: Ensure fasten all connectors securely together.



Step2: Tightly wrap two layers of self-bonding insulating tape (tapes from well-known brands are recommended) forward and backward over the physical connection extending 2 inches beyond the connectors or the end of heat-shrinkable tubing on the RF coaxial cable or omni-antenna connector, and overlapping the tape on each turn.


Wrap two layers of insulating tape on connectors to ensure waterproof
Wrap insulating tape around PoE cable connector and put the cap on console connector

Chapter 4. Basic Configurations

This chapter introduces SMT of Aphelion 3300AG

4.1. Aphelion System Menu Tree (SMT)

Aphelion 3300AG main menu of the SMT will appear after entering correct password of Aphelion 3300AG (the default password is 0000).

```
                Aphelion Communications Inc.
                   Aphelion 3300 Main Menu

General Configuration                 System Management
  11.System General Setup               31.Configuration Management
  12.Interface Configuration            32.Security File Management
  13.Assign WAN Interface               33.Firmware Upgrade
  14.Routing Configuration              34.System reboot

Advanced setting                      System Monitoring
  21.System Password                    41.Interface Link Status
  22.Bandwidth Control                  42.Connecting Client List
  23.DHCP Configuration                 43.System log
  24.NAT Configuration                  44.System Information
  25.SNMP Configuration                 45.Command Line
  26.Wireless Security Setting          99.Logout

                Enter Menu Selection Number :
```

The main menu is organized into 4 major functions:

- General Configuration
- Advanced Setting
- System Management
- System Monitoring

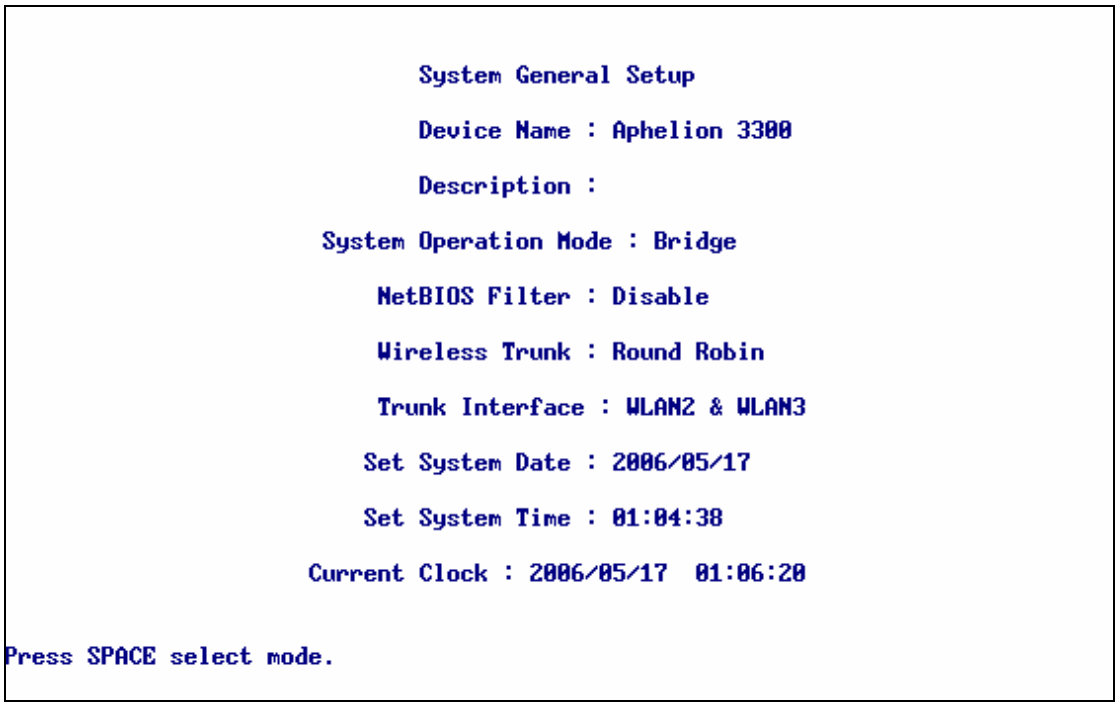
The following sections outline each selection item.

4.2. General Configuration

The General configuration consists of four major parts:

11. System General Setup
12. Interface Configuration
13. Assign WAN interface
14. Routing Configuration

11. System General Setup


System General Setup
Device Name : Aphelion 3300
Description :
System Operation Mode : Bridge
NetBIOS Filter : Disable
Wireless Trunk : Round Robin
Trunk Interface : WLAN2 & WLAN3
Set System Date : 2006/05/17
Set System Time : 01:04:38
Current Clock : 2006/05/17 01:06:20
Press SPACE select mode.

- Device Name & Description
  For identifying a particular outdoor access point.

- System Operation Mode
  Aphelion AP can operate in either bridge mode or router mode. Note that when the AP is configured to operate in bridge mode, all four interfaces operate as bridge. When it is operating in route mode, all four interfaces have its own IP address.

- NetBIOS Filter (available in firmware 0.983 onward)
  When enabled, each client cannot be seen on MicroSof Network Neighborhood.

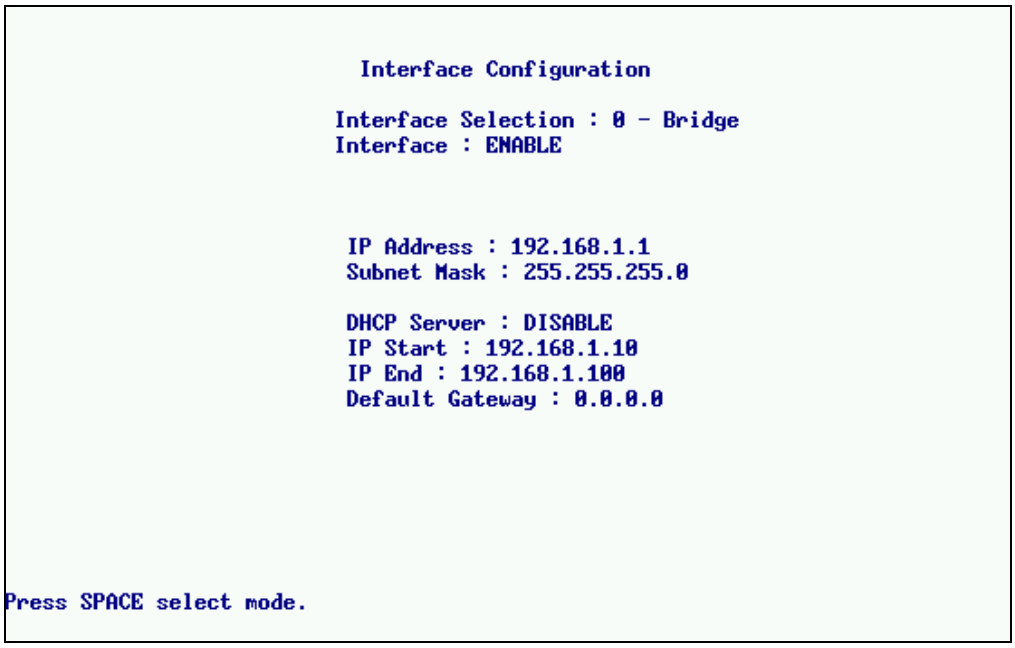
- Wireless Trunk
  Select different wireless trunking mode, namely Round Robin, Load Balance, One-way Transmit and Fail-over, to meet the system requirement.

- Trunk Interface
  Select the combination of wireless interfaces for trunking.

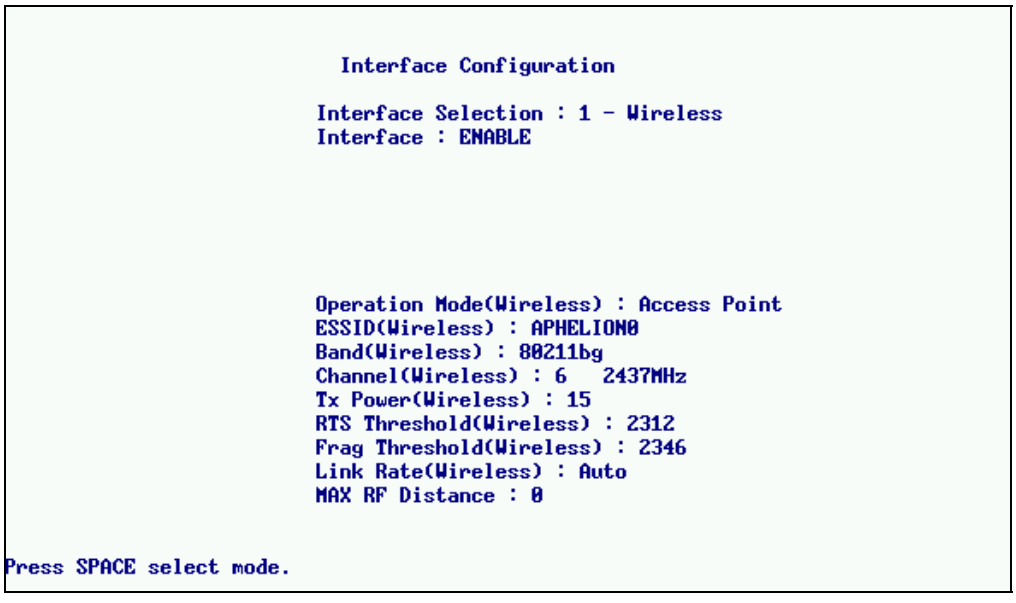
- Set System Date & Set System Time
  Set the date and time
- Current Clock
  Indicating the current clock of the AP (set by user).

12. Interface Configuration

SMT-12 is for configuring the Ethernet interface and three wireless interfaces in Aphelion 3300AG. All physical settings of interfaces are configured here. Each interface can be individually enabled/disabled. Note the message displayed at lower left-hand corner for more information for each selection item.



When 3300AG is configured as a bridge, the IP address of 3300AG is set in the Ethernet interface. Depends on the system, DHCP server and gateway can also be set in SMT-12. When 3300AG is configured as a router, the interface configuration looks slightly different and its DHCP is set in SMT-23 DHCP Configuration, and the gateway is set in SMT-13 Assign WAN interface.



The following settings can be configured for the wireless interface :

- Operation Mode
  Wireless interface can be set as an access point (AP) or a wireless station (also called AP client (AC)). When the interface is an AP, it accepts connection requests from wireless clients, such as wireless internet cards in PC or WiFi phones. When the interface is a wireless station, it looks for the AP with the same ESSID to connect. It will not accept any connection request from other wireless clients.

- ESSID/MESSID (available in Firmware 0.983 onward)
  Assign ESSID to the interface for connection identification. Multiple ESSID (MESSID) can be assigned by pressing right key. Up to eight different ESSID can be assigned for each wireless interface.

- Band
  Select between 2.4GHz 802.11b/g or 5GHz 802.11a.

- Channel
  Operation channel for the wireless interface. When the interface is set as a wireless station, selecting Channel 0 AUTO let the interface automatically detect the appropriate channel used by the AP with the same ESSID.

- Tx Power
  Set the transmit power of the interface (the RF card).

- RTS Threshold
  Setting the packet size to trigger RTS/CTS enable. This is normally set in AC side only because the hidden station problem does not exit from the perspective of the AP. RTS Threshold can be set between 1 and 2312 bytes.

- Frag Threshold
  Setting the packet size to activate fragmentation. Frag Threshold can be set between 1 and 2312 bytes.

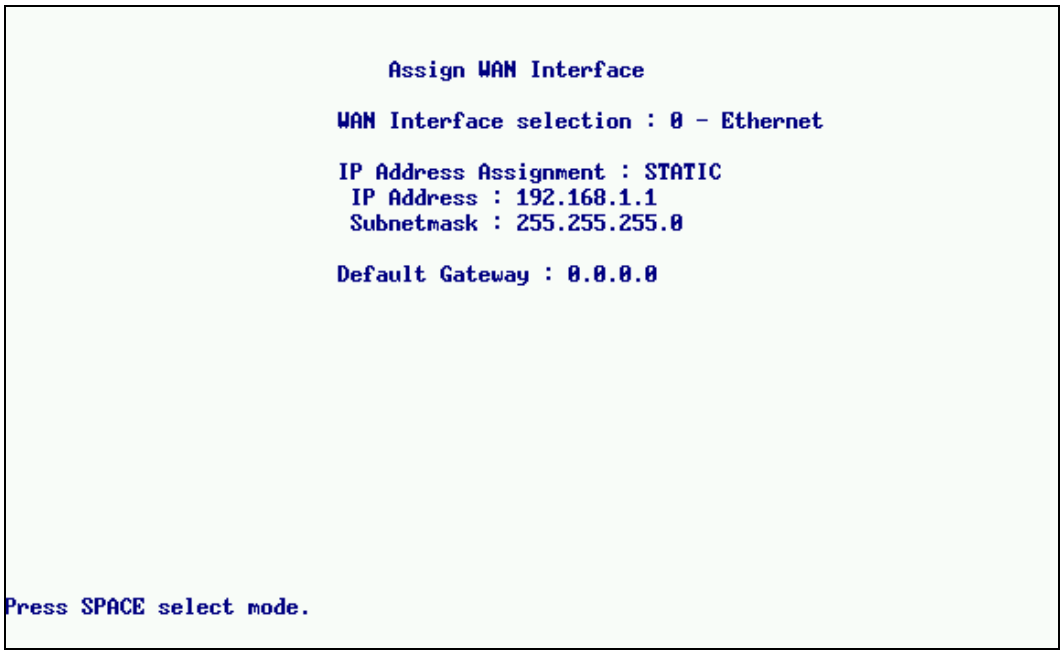
- Link Rate
  Set the data link rate for 3300AG. When it is set to AUTO, 3300AG will use the maximum possible rate to transmit the data.

- MAX RF Distance
  3300AG can adjust the TTL of packets according to the given distance to improve the communication quality. It is recommended to set MAX RF

Distance when the distance of point to point connection is greater than 7km.

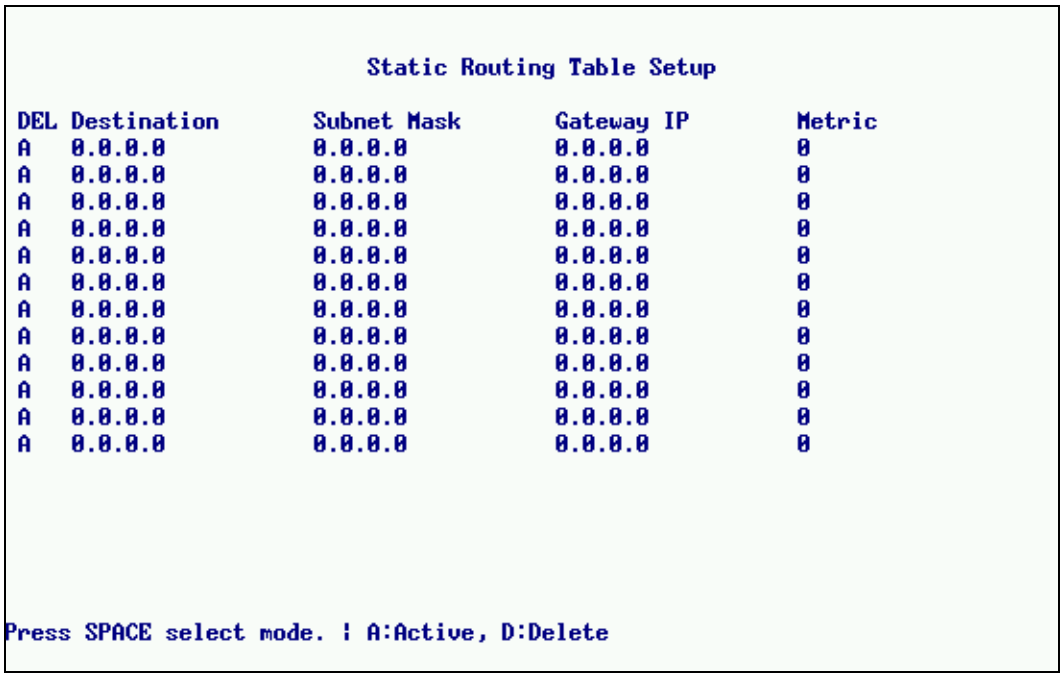
In addition, when 3300AG is operating in Router Mode, each interface can be individually assigned IP address and gateway.

13. Assign WAN Interface


Assign WAN Interface
WAN Interface selection : 0 - Ethernet
IP Address Assignment : STATIC
IP Address : 192.168.1.1
Subnetmask : 255.255.255.0
Default Gateway : 0.0.0.0
Press SPACE select mode.

This is only available when 3300AG is operating in router mode to assign gateway. Any one of the four interfaces can be specified as WAN.

14. Routing Configuration



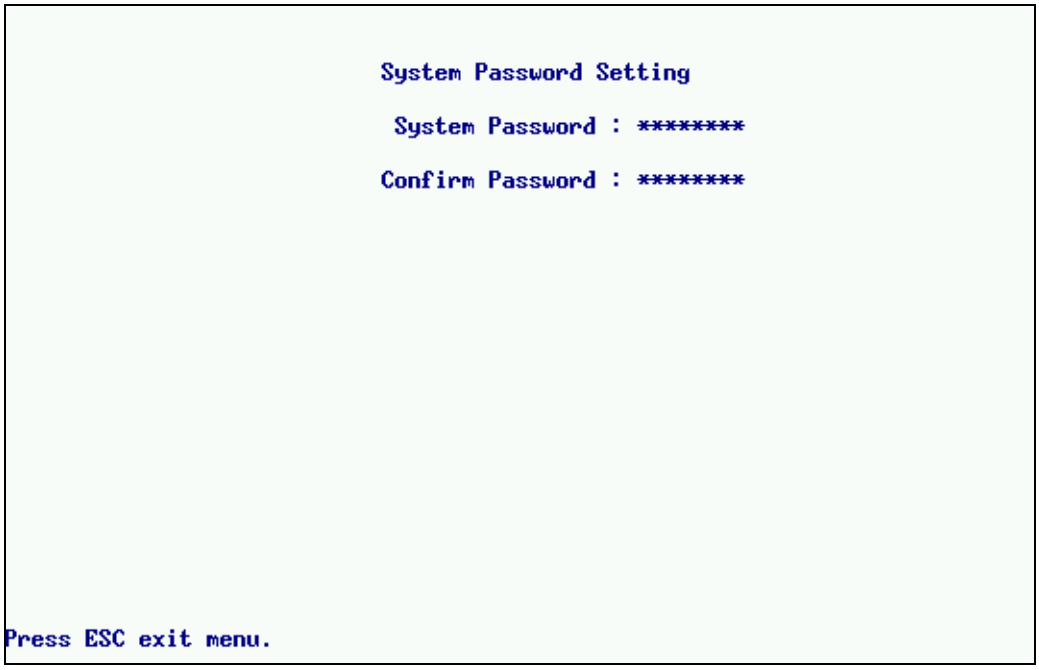
Up to 12 rules of static routes can be configured here.

4.3. Advanced Setting

Under advanced settings, you will be able to configure the following:

21. System Password
22. Bandwidth Control
23. DHCP Configuration
24. NAT Configuration
25. SNMP configuration
26. Wireless Security Setting

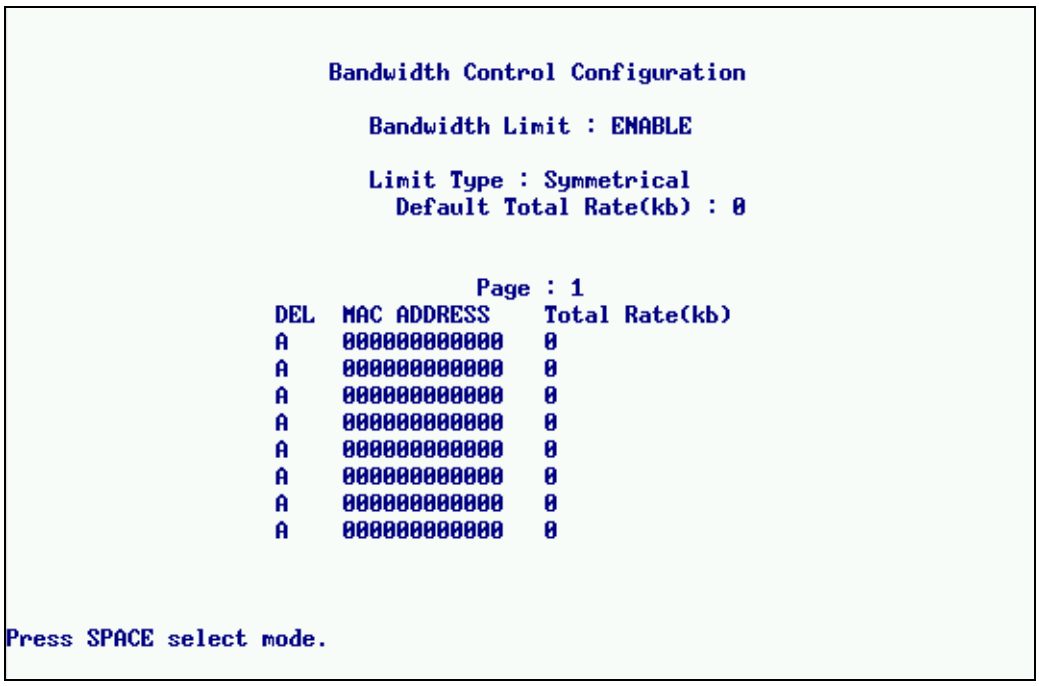
21. System Password

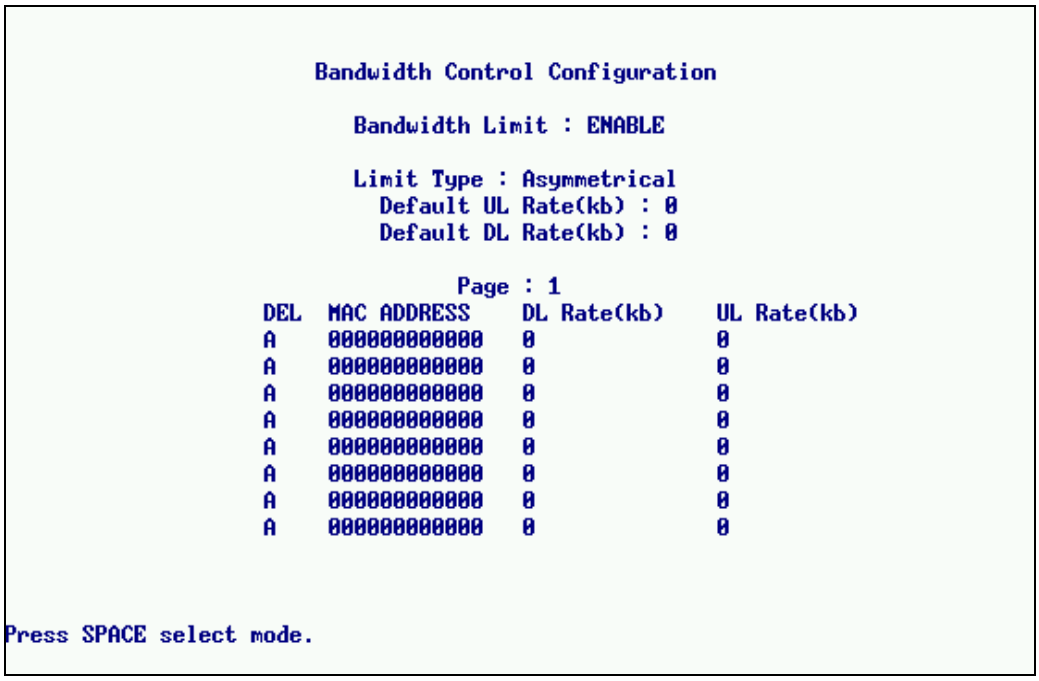


The default password to access Aphelion 3300AG SMT is 0000. SMT-21 enables users to change the password of 3300AG. The new password will take in place on the next login.

In the case of forgotten password, the only way to enter SMT is by hard resetting the 3300AG to factory default, detailed in Chapter 5 of this manual. However, hard reset will erase all the configurations that had on the 3300AG and make all the settings back to factory default.

22. Bandwidth Control



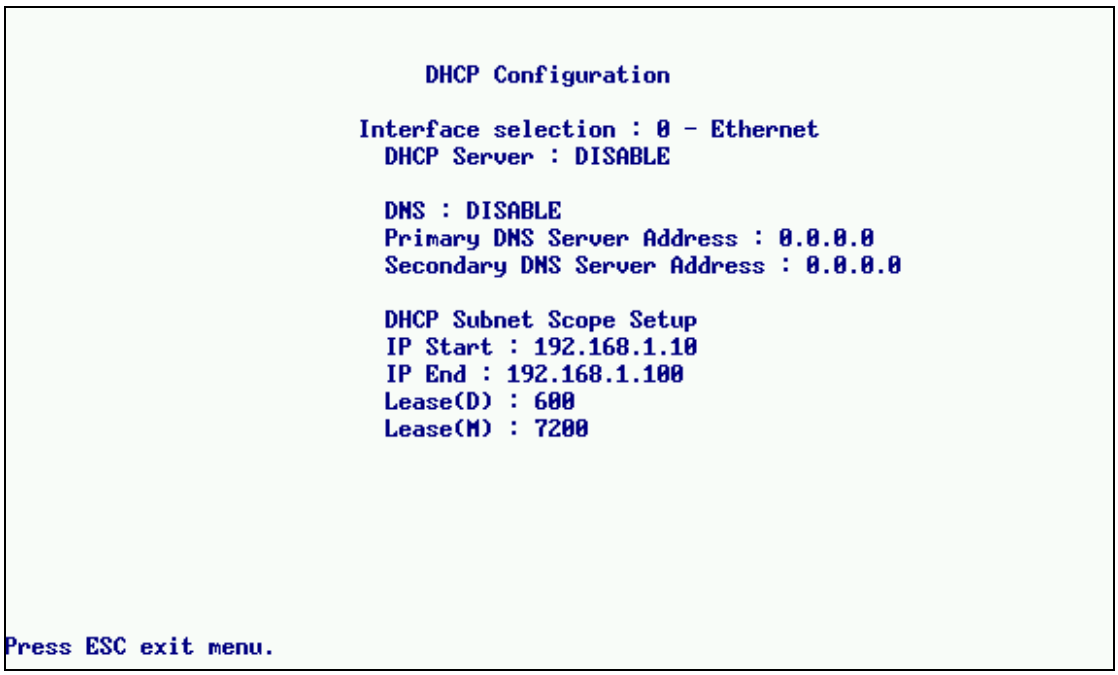

Bandwidth Control Configuration
Bandwidth Limit : ENABLE
Limit Type : Asymmetrical
Default UL Rate(kb) : 0
Default DL Rate(kb) : 0
Page : 1
DEL MAC ADDRESS DL Rate(kb) UL Rate(kb)
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
A 000000000000 0 0
Press SPACE select mode.

Downstream and upstream data rates for subscriber or the client devices connecting to 3300AG can be defined here. There are two types of bandwidth limit in Aphelion 3300AG. Symmetrical bandwidth limit consolidates download and upload rate of each individual client connection. Asymmetrical bandwidth limit specifies download and upload rate of client connections. Once the bandwidth limit is enabled, the limitation applies to all clients that connect to the 3300AG.

For specific client connections, Aphelion system provides a table for network administrator to limit bandwidth of each individual client by MAC address. Once

these client MAC addresses are set in the table, the general bandwidth limit rule will not apply to the connection of devices with these MAC address. Only the specified bandwidth limit rule applied.

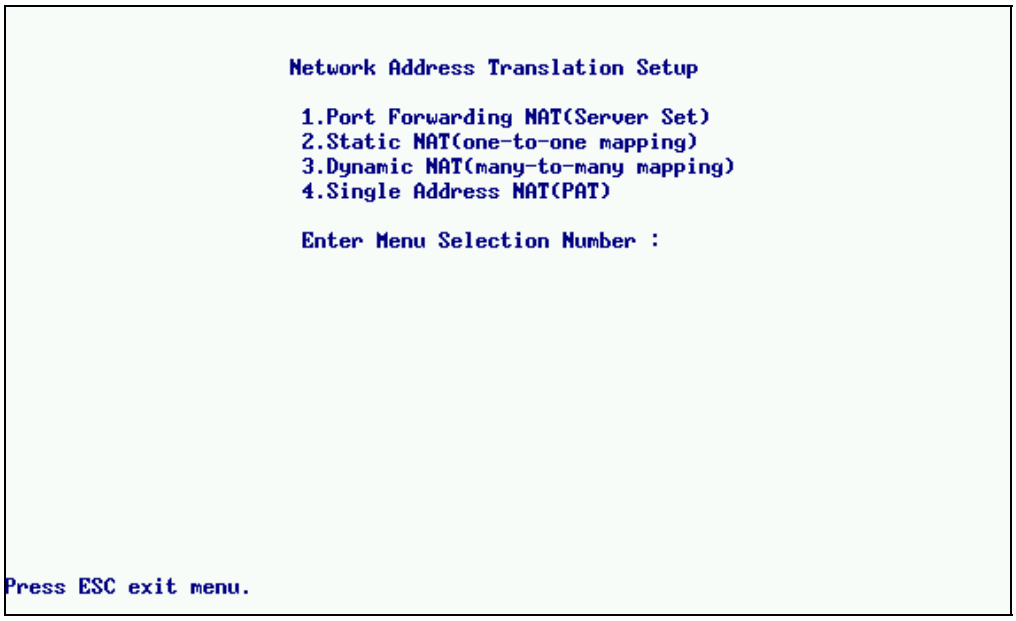
23. DHCP Configuration


DHCP Configuration
Interface selection : 0 - Ethernet
DHCP Server : DISABLE
DNS : DISABLE
Primary DNS Server Address : 0.0.0.0
Secondary DNS Server Address : 0.0.0.0
DHCP Subnet Scope Setup
IP Start : 192.168.1.10
IP End : 192.168.1.100
Lease(D) : 600
Lease(M) : 7200
Press ESC exit menu.

The scope of DHCP client pool that corresponds to the selected interface and subnet are defined in this menu. Lease (D) is the duration that the DHCP server grants to the DHCP client permission to use a particular IP address. Lease (M) is the maximum lease time.

Each Ethernet or wireless interface can be the gateway of its own subnet. Hence there can be three subnet domains in one Aphelion 3300AG in routing mode. This DHCP configuration is only available when 3300AG is operating in router mode.

24. NAT Configuration

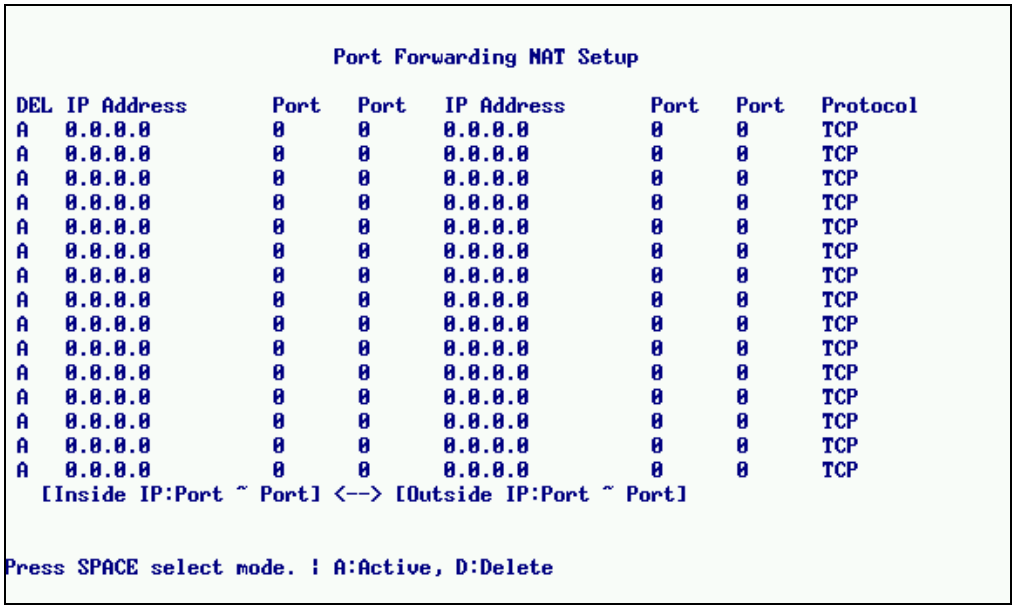


Network Address Translation can be setup in four different ways :

1. Port forwarding NAT (Server sets)
2. Static NAT (One to One Mapping)
3. Dynamic NAT (Many to Many Mapping)
4. Single Address NAT (PAT)

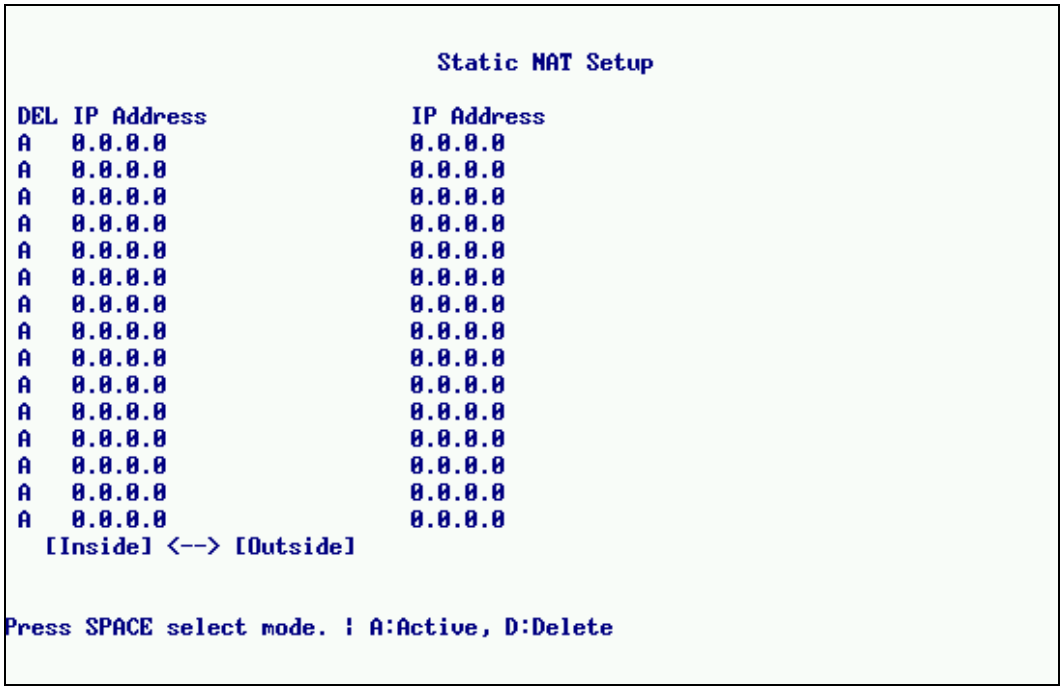
This configuration in only available when 3300AG is operating in router mode.

Port Forwarding


Port Forwarding NAT Setup
DEL IP Address Port Port IP Address Port Port Protocol
A 0.0.0.0 0 0 0.0.0.0 0 0 TCP
[Inside IP:Port ~ Port] <--> [Outside IP:Port ~ Port]
Press SPACE select mode. ! A:Active, D:Delete

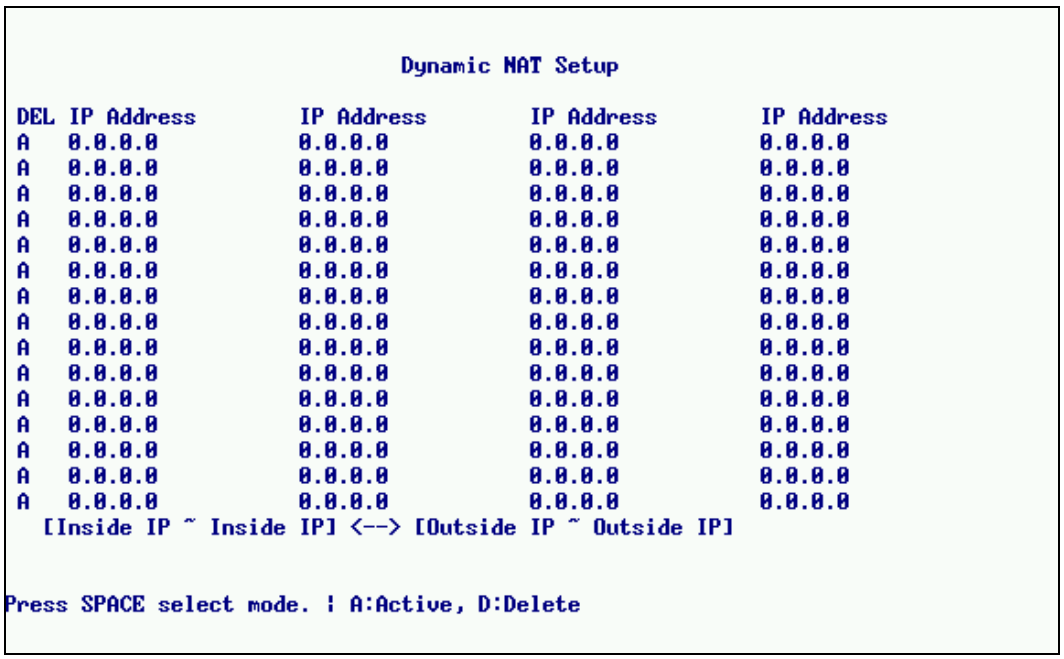
Server sets where internal IP addresses are mapped according to the TCP or UDP port are defined in this Port Forwarding NAT sub-menu.

Static NAT



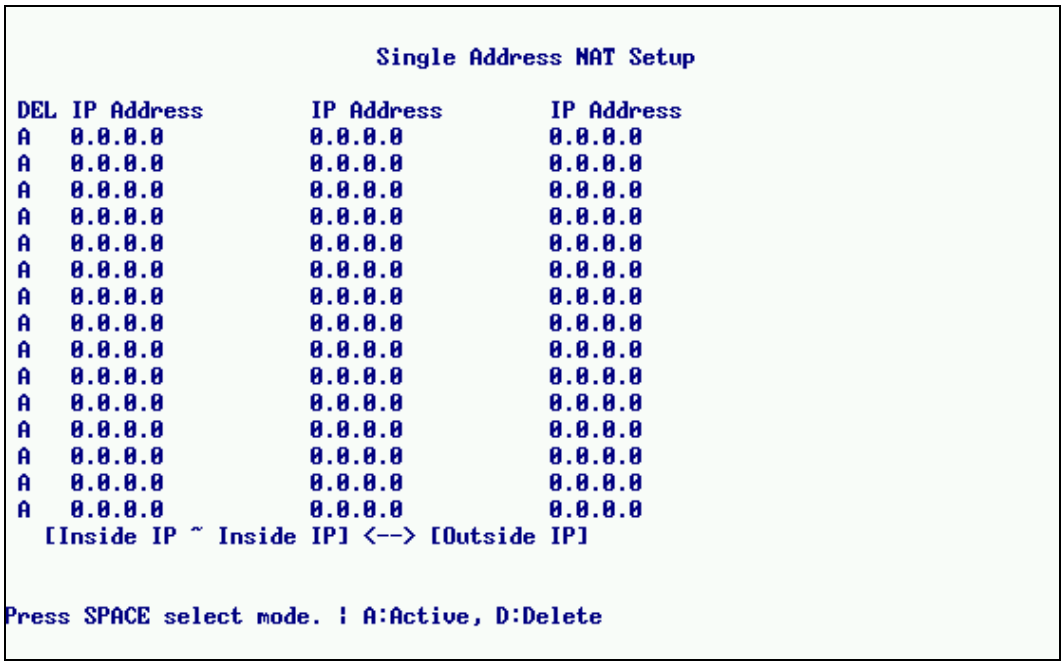
In this menu, you will be able to map internal private IP address to a global WAN IP address.

Dynamic NAT


Dynamic NAT Setup
DEL IP Address
IP Address
IP Address
IP Address
A 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
[Inside IP ~ Inside IP] <--> [Outside IP ~ Outside IP]
Press SPACE select mode. ¦ A:Active, D:Delete

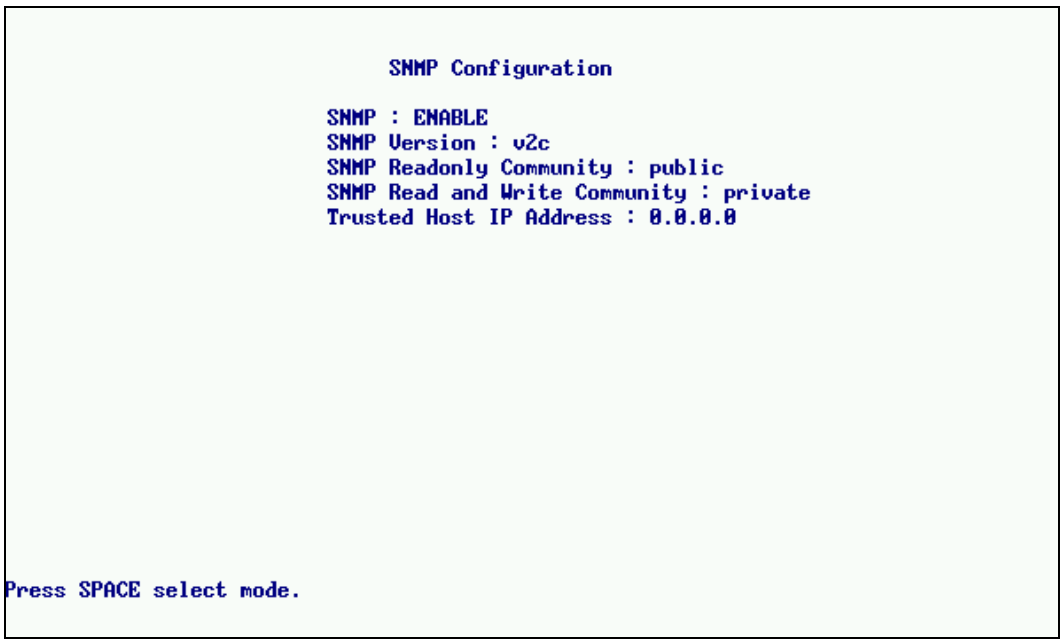
A range of internal IP address can be mapped to a range of global IP address.

Single Address (NAT/PAT)


Single Address NAT Setup
DEL IP Address IP Address IP Address
A 0.0.0.0 0.0.0.0 0.0.0.0
[Inside IP ~ Inside IP] <--> [Outside IP]
Press SPACE select mode. ¦ A:Active, D:Delete

A range of internal IP addresses can be mapped to a single global WAN IP addresses here.

25. SNMP configuration


SNMP Configuration
SNMP : ENABLE
SNMP Version : v2c
SNMP Readonly Community : public
SNMP Read and Write Community : private
Trusted Host IP Address : 0.0.0.0
Press SPACE select mode.

SNMP is configured here for simple network management. Aphelion 3300AG supports all SNMP v1, v2 and v3. Aphelion has experience working with ILECs, CLECs, WISPs and MSOs, for customized MIB requirements, please contact support@aphelions.com for assistance.

26. Wireless Security Setting

Comprehensive security settings are available on Aphelion 3300AG in this menu.

These include Hide ESSID, WEP Keys, 802.1x EAP-TLS, 802.1x EAP-MD5, WPA-PSK, WPA-EAP, MAC Address Filtering and RADIUS. Details of each type of security are in appendix. The security setting of each wireless interface is configured separately. Note the message at the bottom of SMT page for information on each selection items.

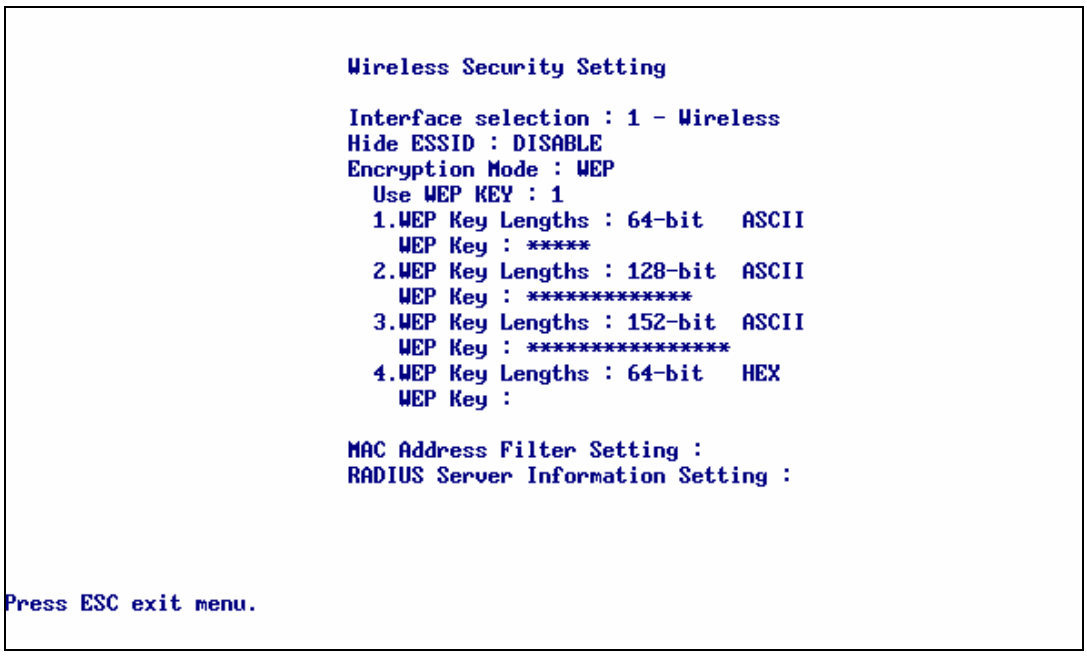
- Hide ESSID

  When Hide ESSID is enabled, the ESSID of an AP will not be seen so only the authorized AC knows the existence of the AP. This prevents an unexpected client connecting to the AP.

- WEP

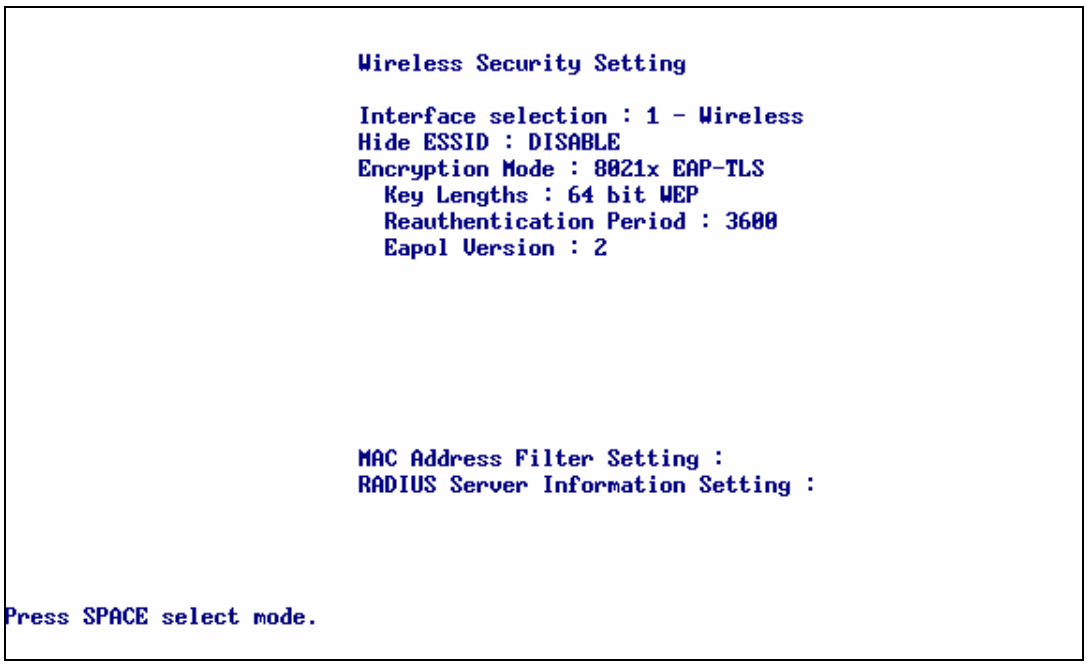
  Aphelion 3300AG supports 64-bit, 128-bit and 152-bit WEP key in both ASCII and HEX format. Do make sure the correctly number of digits/characters and format of WEP key as shown in the table are entered. Note that in HEX format, HEX number cannot start with “0”. An error message will appear upon exiting SMT-26 when an illegal WEP key is entered.

Number of digit/character	ASCII	HEX
64-bit	5	10
128-bit	13	26
152-bit	16	32


Wireless Security Setting
Interface selection : 1 - Wireless
Hide ESSID : DISABLE
Encryption Mode : WEP
Use WEP KEY : 1
1.WEP Key Lengths : 64-bit ASCII
WEP Key : *****
2.WEP Key Lengths : 128-bit ASCII
WEP Key : **********
3.WEP Key Lengths : 152-bit ASCII
WEP Key : **********
4.WEP Key Lengths : 64-bit HEX
WEP Key :
MAC Address Filter Setting :
RADIUS Server Information Setting :
Press ESC exit menu.

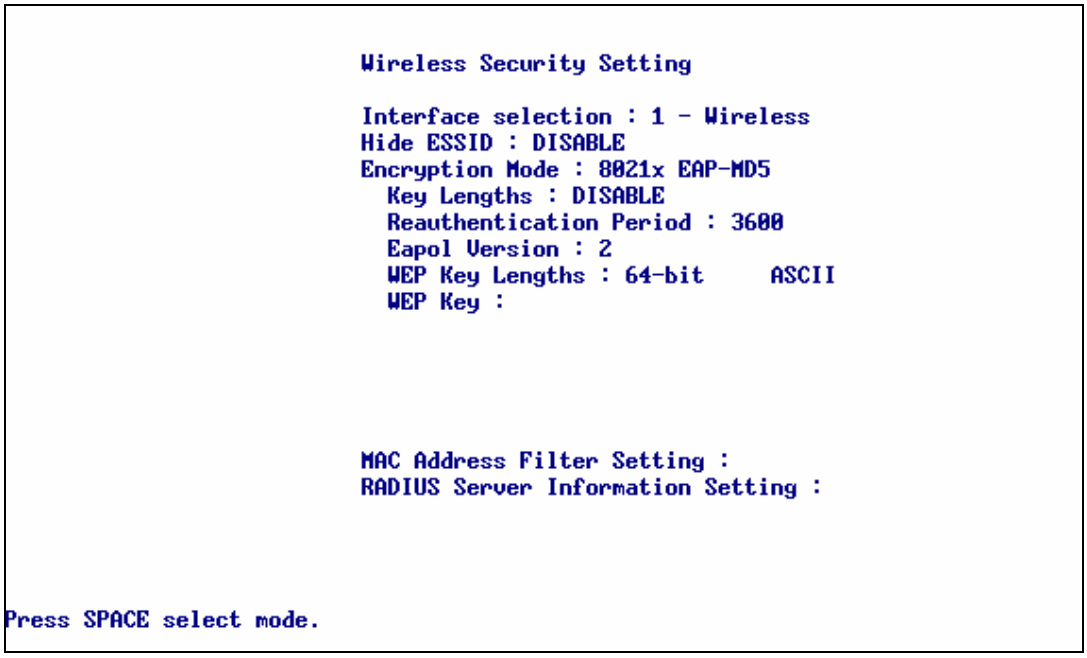
- 802.1x EAP-TLS

  Both 64-bit and 128-bit WEP can be set for reauthentication period up to 65535 bytes. Two Eapol (EAP over LAN) versions are available.


Wireless Security Setting
Interface selection : 1 - Wireless
Hide ESSID : DISABLE
Encryption Mode : 8021x EAP-TLS
Key Lengths : 64 bit WEP
Reauthentication Period : 3600
Eapol Version : 2
MAC Address Filter Setting :
RADIUS Server Information Setting :
Press SPACE select mode.

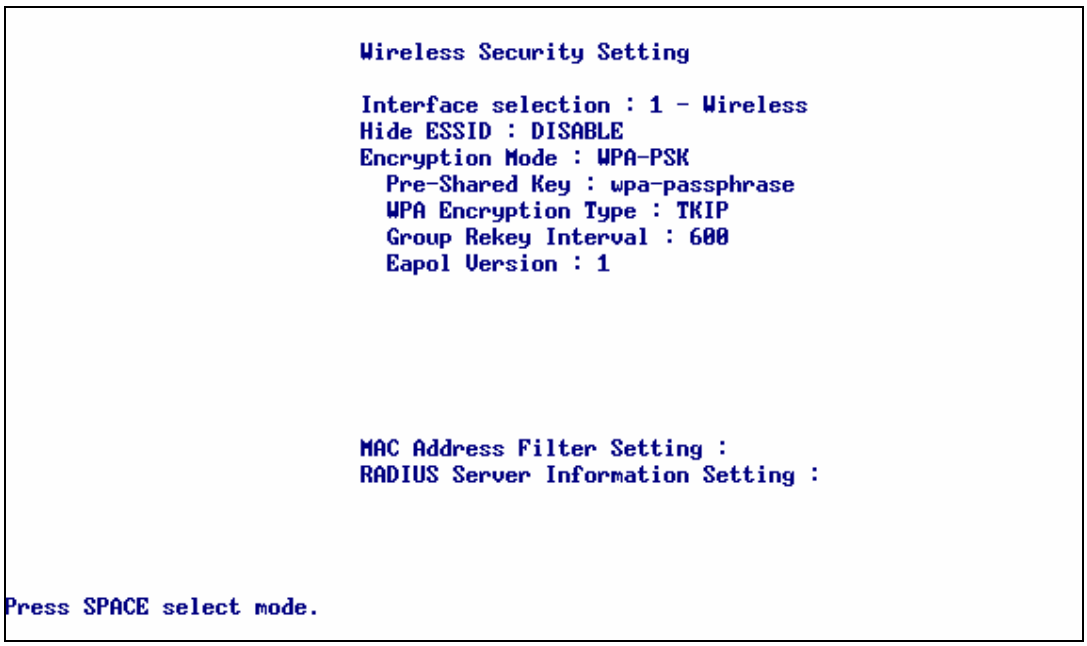
- 802.1x EAP-MD5

  WEP Key of 64-bit, 128-bit and 152-bit in both ASCII and HEX format can be set for EAP-MD5. Two Eapol version are available with reauthentication period of up to 65535 bytes.


Wireless Security Setting
Interface selection : 1 - Wireless
Hide ESSID : DISABLE
Encryption Mode : 8021x EAP-MD5
Key Lengths : DISABLE
Reauthentication Period : 3600
Eapol Version : 2
WEP Key Lengths : 64-bit ASCII
WEP Key :
MAC Address Filter Setting :
RADIUS Server Information Setting :
Press SPACE select mode.

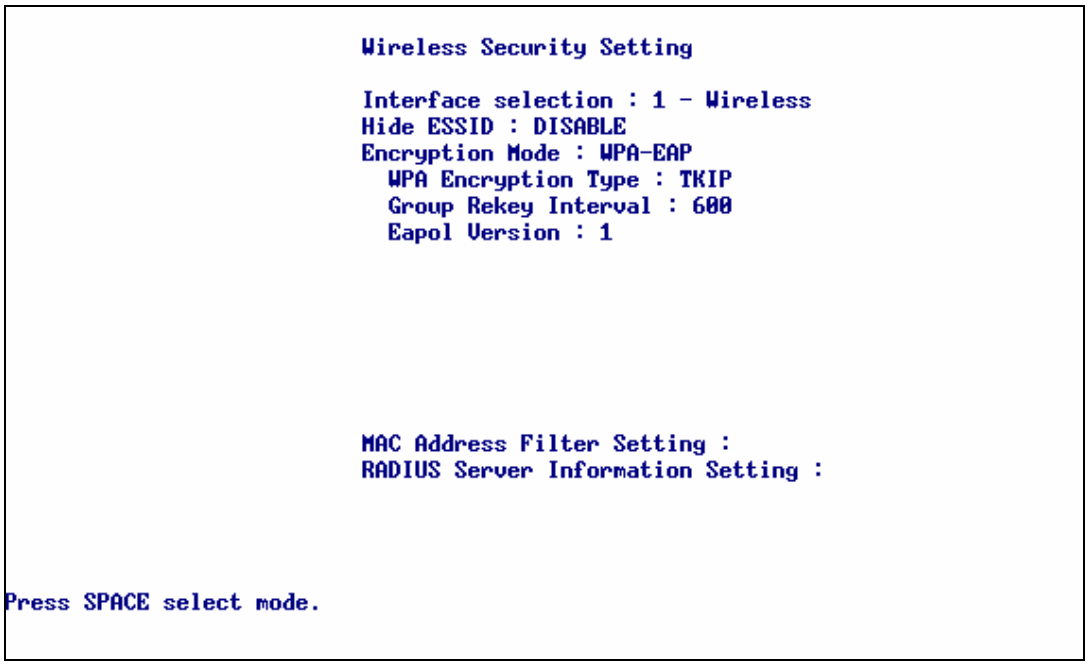
- WPA-PSK

  Both TKIP and CCMP encryption are available for WPA-PSK. Pre-shared key of 8 to 63 characters are required. Group Rekey Interval can be set up to 65536 bytes. Two Eapol version are available.


Wireless Security Setting
Interface selection : 1 - Wireless
Hide ESSID : DISABLE
Encryption Mode : WPA-PSK
Pre-Shared Key : wpa-passphrase
WPA Encryption Type : TKIP
Group Rekey Interval : 600
Eapol Version : 1
MAC Address Filter Setting :
RADIUS Server Information Setting :
Press SPACE select mode.

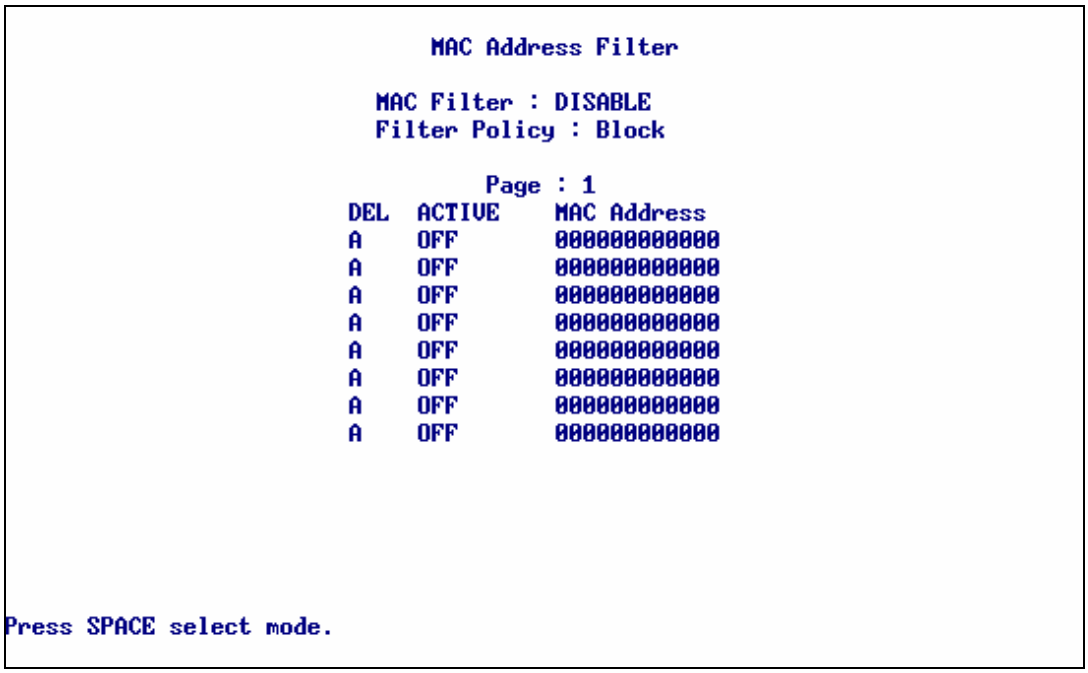
- WPA-EAP

  Both TKIP and CCMP encryption are available for WPA-EAP. Pre-shared key of 8 to 63 characters are required. Group Rekey Interval can be set up to 65536 bytes. Two Eapol version are available.


Wireless Security Setting
Interface selection : 1 - Wireless
Hide ESSID : DISABLE
Encryption Mode : WPA-EAP
WPA Encryption Type : TKIP
Group Rekey Interval : 600
Eapol Version : 1
MAC Address Filter Setting :
RADIUS Server Information Setting :
Press SPACE select mode.

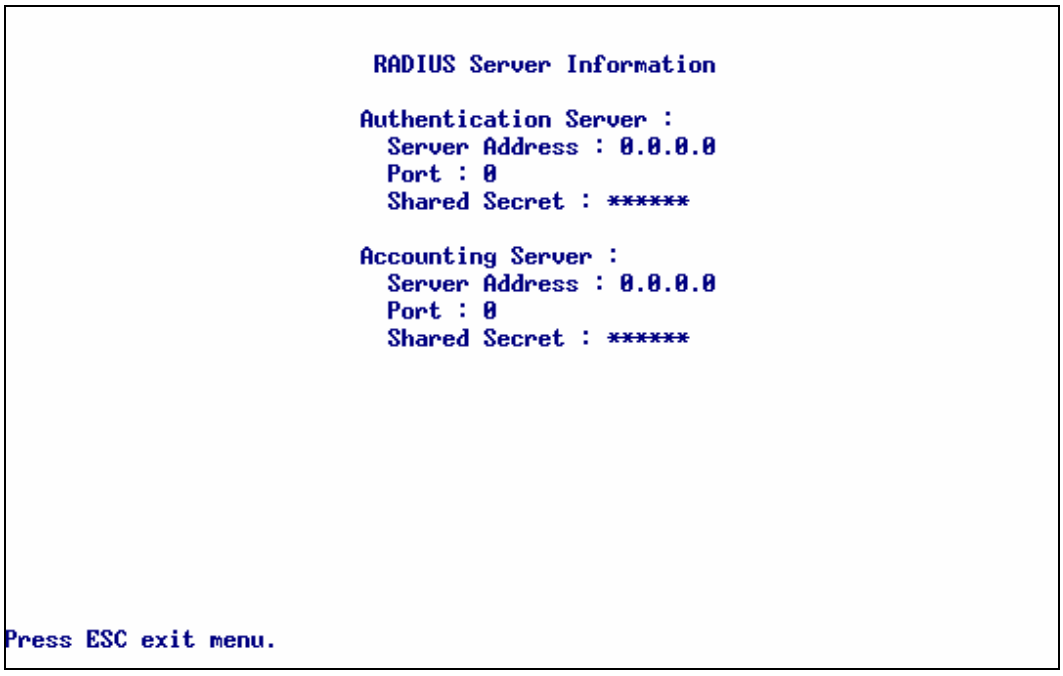
- MAC Address Filtering

  Aphelion 3300AG can control the client connection by accepting or blocking the traffic from devices of specific MAC addresses.



- RADIUS

RADIUS settings for 802.1x protocol authenticating with the remote RADIUS server for authenticating, authorization and accounting are set in this menu.



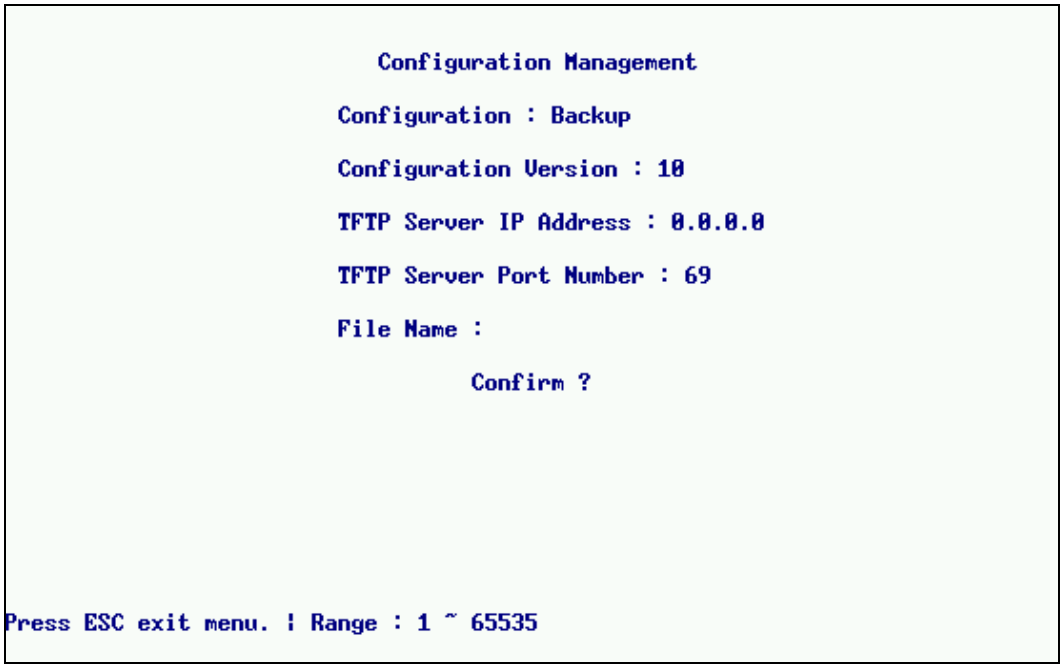
4.4. System Management

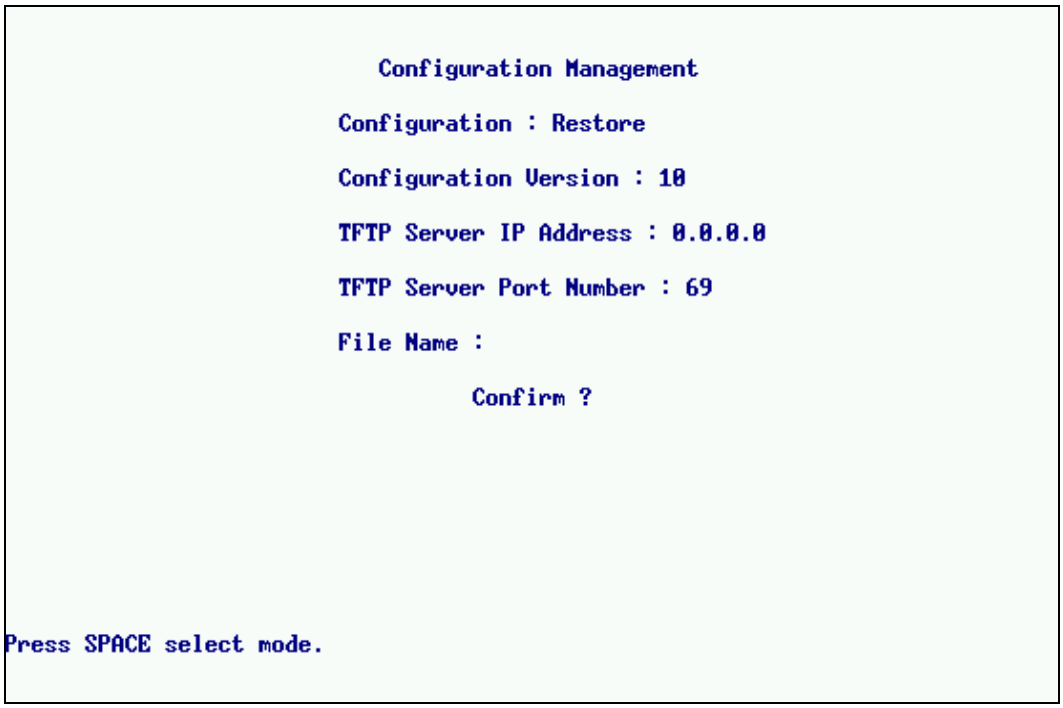
Under System Management, you will be able to operate the system by following:

31. Configuration Management
32. Security File Management
33. Firmware Upgrade
34. System reboot

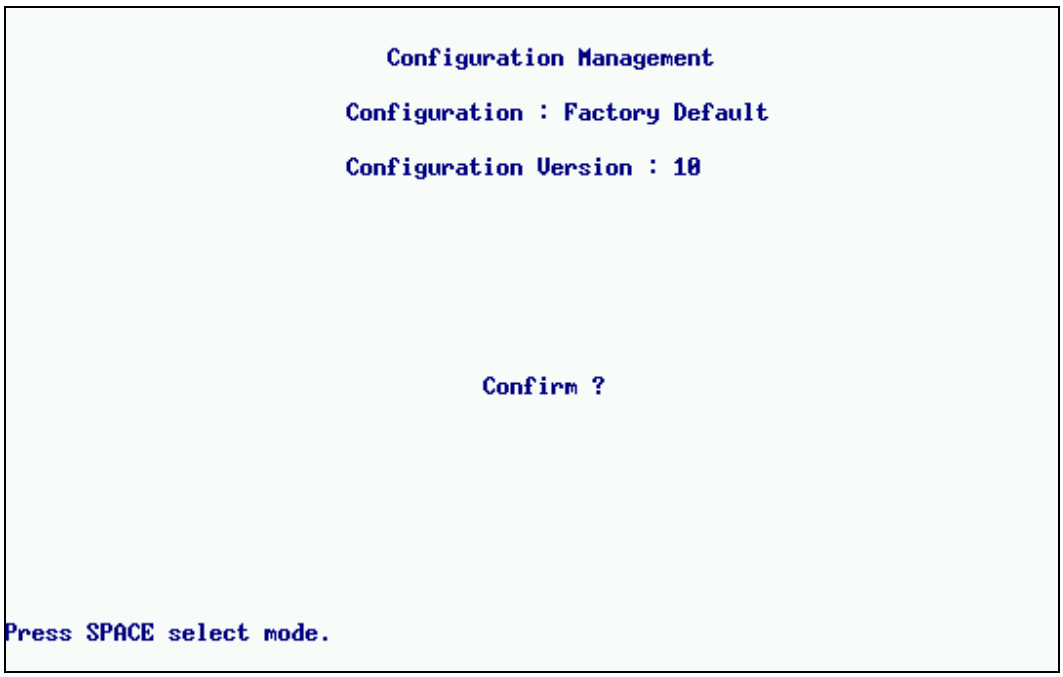
31. Configuration management

The configuration of 3300AG can be backed-up or restored by using TFTP here. In a daisy chained sequential configurations, it is recommended to backup all configurations before uploading/upgrading firmware. You may name your configuration file in any ways you like.

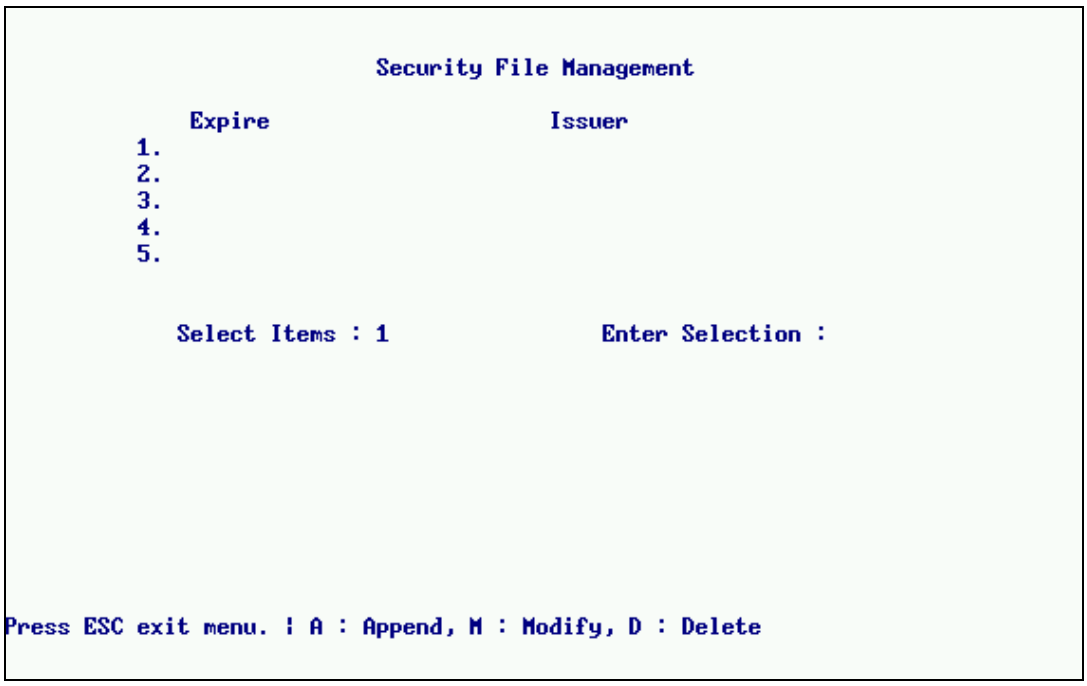

Configuration Management
Configuration : Backup
Configuration Version : 10
TFTP Server IP Address : 0.0.0.0
TFTP Server Port Number : 69
File Name :
Confirm ?
Press ESC exit menu. ! Range : 1 ~ 65535

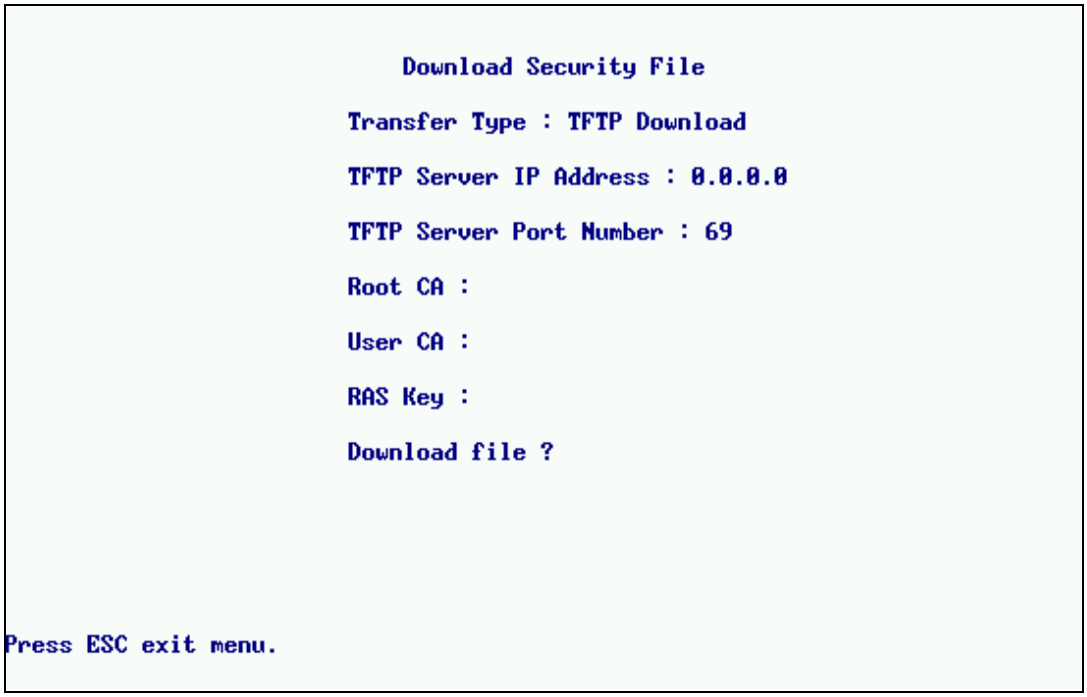


The configuration of Aphelion 3300AG can be reset to factory default by using this menu.



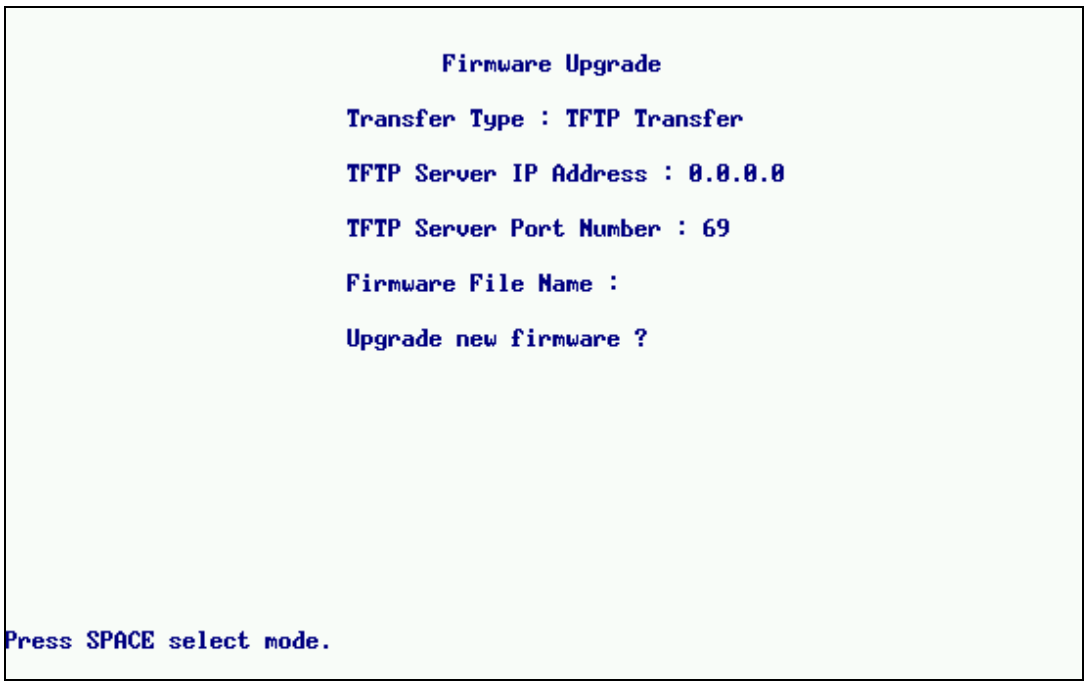
32. Security File Management

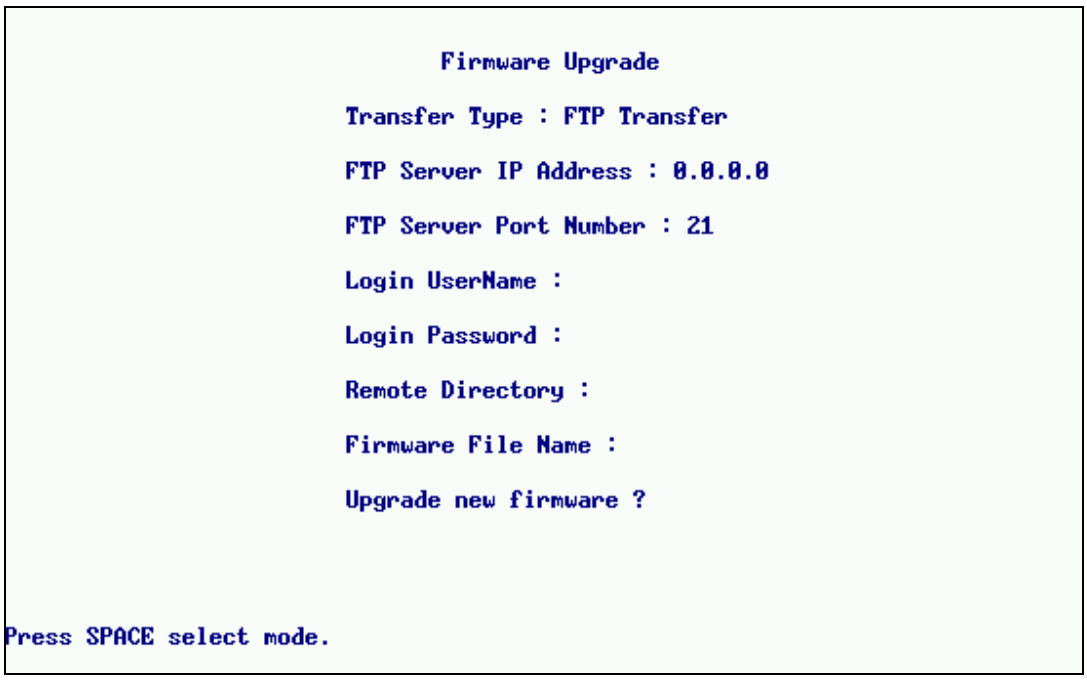



Download Security File
Transfer Type : TFTP Download
TFTP Server IP Address : 0.0.0.0
TFTP Server Port Number : 69
Root CA :
User CA :
RAS Key :
Download file ?
Press ESC exit menu.

For running EAP_TLS secure connection, network administrators may need to upload User Certificate, Root Certificate and RSA Key file to the system. In this menu, system allows administrators to upload these Certificate files with TFTP server to the access point. Please refer to Appendix for more on wireless security.

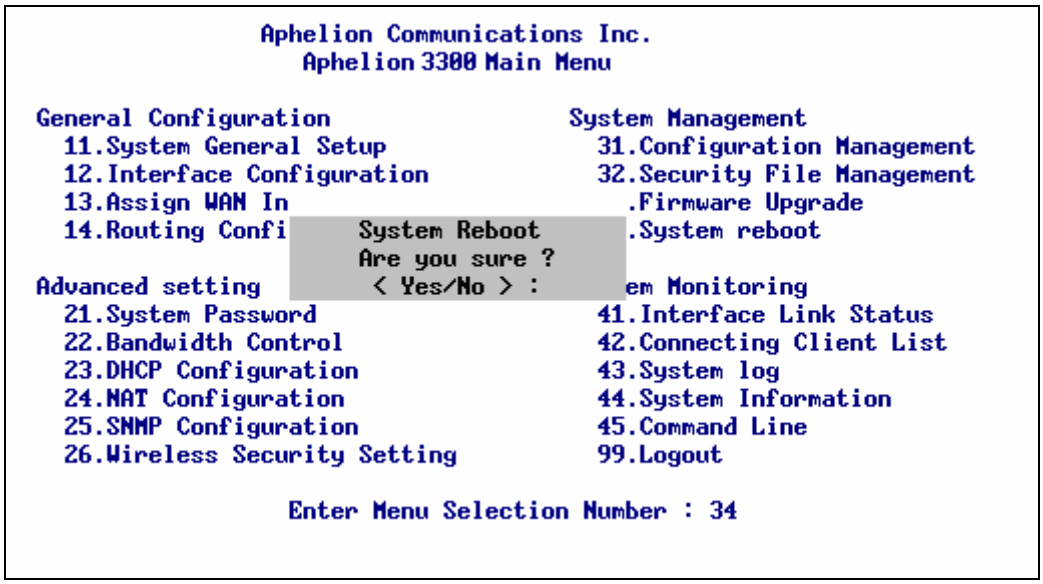
33. Firmware Upgrade


Firmware Upgrade
Transfer Type : TFTP Transfer
TFTP Server IP Address : 0.0.0.0
TFTP Server Port Number : 69
Firmware File Name :
Upgrade new firmware ?
Press SPACE select mode.


Firmware Upgrade
Transfer Type : FTP Transfer
FTP Server IP Address : 0.0.0.0
FTP Server Port Number : 21
Login UserName :
Login Password :
Remote Directory :
Firmware File Name :
Upgrade new firmware ?
Press SPACE select mode.

New firmware can be uploaded to 3300AG by either TFTP or FTP. Upgrading firmware from FTP server may need username and password for login. After the firmware has been loaded onto 3300AG, the upgrading progress will show on the menu. **Please do not shutdown the system during the upgrading process to prevent unexpected system failure**. System will automatically reboot and perform firmware image backup after the upgrade. New firmware will take effect after another system reboot. Please refer to application note on firmware upgrade for step by step upgrading process.

34. System Reboot



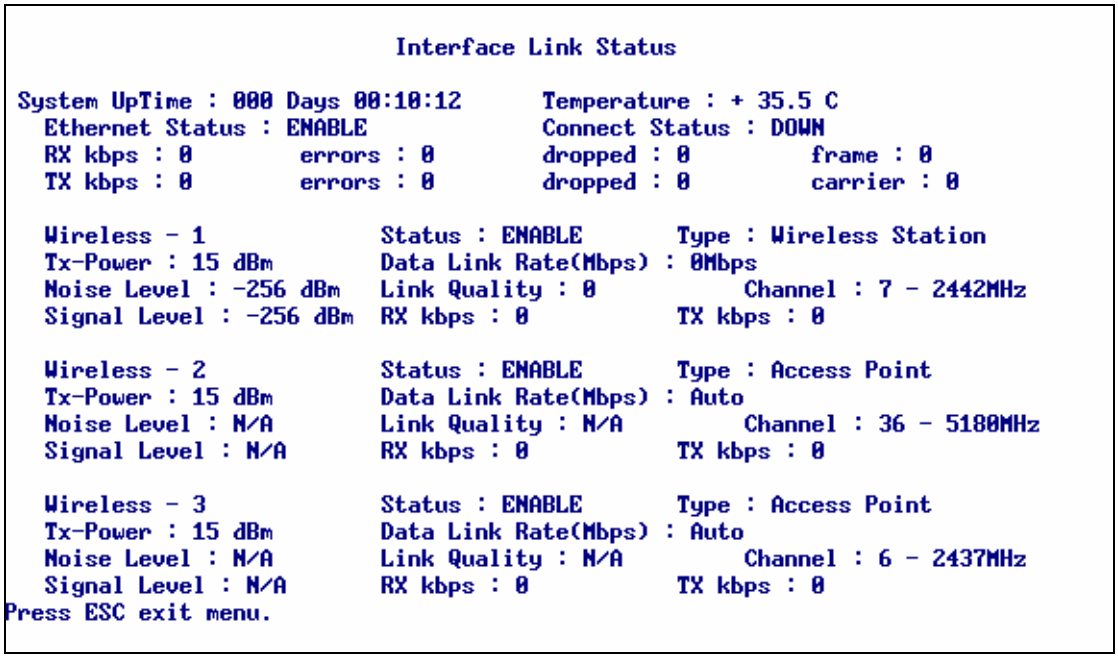
Reboot 3300AG from SMT without disconnecting power cable or changing any connection. Certain configurations require system reboot to take place, such as configuration restore.

4.5. System Monitoring

SMT-41 ~ 45 provides system monitoring for 3300AG. The following sections introduce each item :

41. Interface Link Status
42. Connecting Client List (Wireless Clients)
43. System log
44. System Information
45. Command Line

41. Interface Link Status


Interface Link Status
System UpTime : 000 Days 00:10:12
Temperature : + 35.5 C
Ethernet Status : ENABLE
Connect Status : DOWN
RX kbps : 0
errors : 0
dropped : 0
frame : 0
TX kbps : 0
errors : 0
dropped : 0
carrier : 0
Wireless - 1
Status : ENABLE
Type : Wireless Station
Tx-Power : 15 dBm
Data Link Rate(Mbps) : 0Mbps
Noise Level : -256 dBm
Link Quality : 0
Channel : 7 - 2442MHz
Signal Level : -256 dBm
RX kbps : 0
TX kbps : 0
Wireless - 2
Status : ENABLE
Type : Access Point
Tx-Power : 15 dBm
Data Link Rate(Mbps) : Auto
Noise Level : N/A
Link Quality : N/A
Channel : 36 - 5180MHz
Signal Level : N/A
RX kbps : 0
TX kbps : 0
Wireless - 3
Status : ENABLE
Type : Access Point
Tx-Power : 15 dBm
Data Link Rate(Mbps) : Auto
Noise Level : N/A
Link Quality : N/A
Channel : 6 - 2437MHz
Signal Level : N/A
RX kbps : 0
TX kbps : 0
Press ESC exit menu.

Real-time link statuses of all interfaces are shown in the menu.

- System Up Time
  Display how long 3300AG has been operating since last boot-up.

- Temperature
  The temperature inside the waterproof housing.

- Interface Status
  Indicate the interface is ENABLE or DISABLE.

- Type
  Indicate the wireless interface is configured as an AP or wireless station.

- Tx-Power
  Transmit power of wireless interface set in SMT-12.

- Data Link Rate
  Real-time data transmission rate. When Data Link Rate in SMT-12 is set, it displays here. Otherwise, when it is set as AUTO in SMT-12, Data Link Rate here indicates the maximum transmission rate available, and can be used as an indication of link quality. The maximum link rate according to 802.11a/g is 54Mbps. Only available when the interface is set as an AC.

- Link Quality
  Calculated from RSSI, signal and noise level to indicate the quality of the

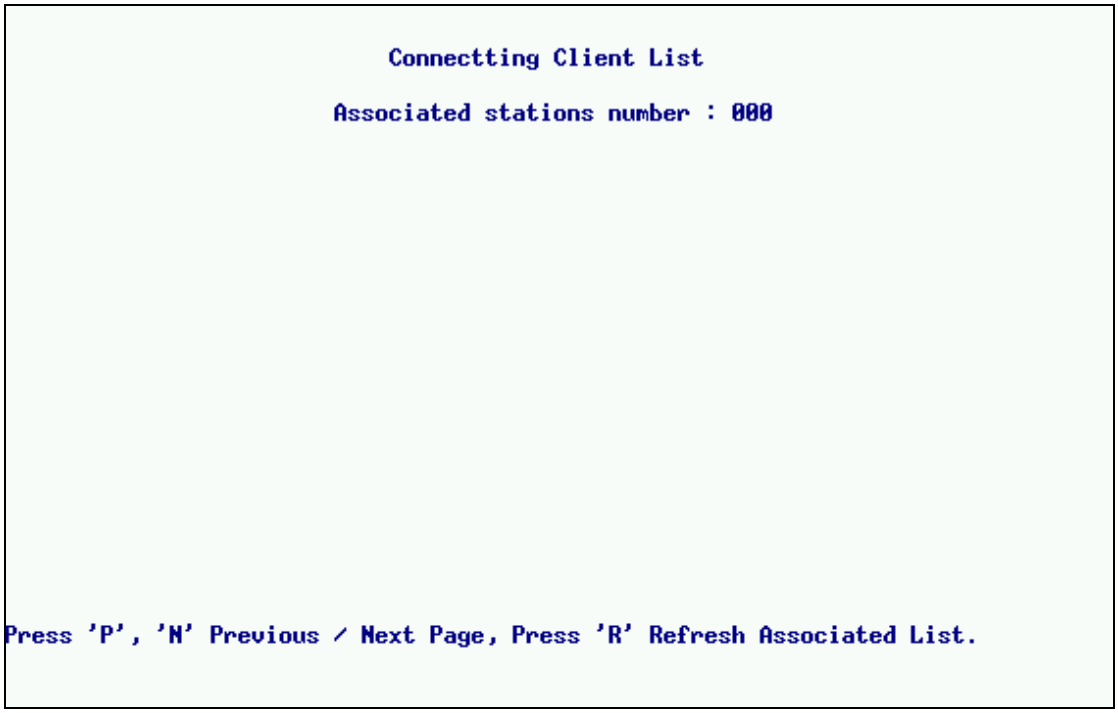
communication link in percentage.

- Channel
  The channel used by the wireless interface.

- Signal Level
  A -70 ~ -50dBm signal level is recommended for a good connection. Too low a signal, the wireless link between AP and AC can not be established. Too high a signal level, the power amplifier at the receiver might be forced to operate in saturation region and distorts the signal waveform. Hence likely to result in reception error. Since the signal level at AP is defined by the user, Signal Level is only available when the interface is set as an AC.

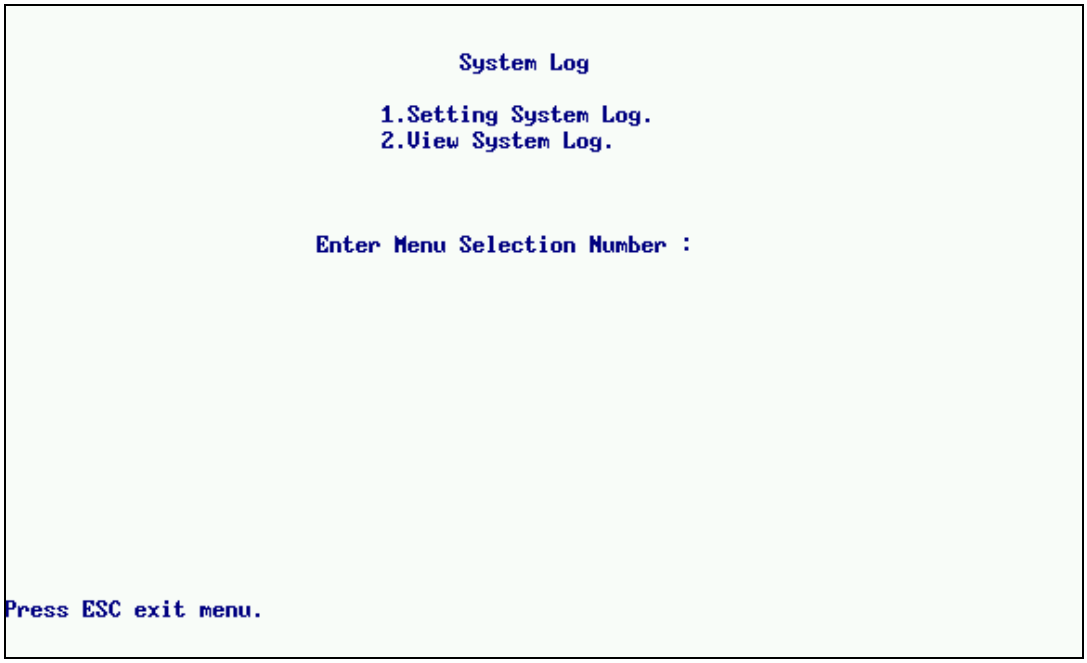
- Noise Level
  Indicate the noise level at the AC end.

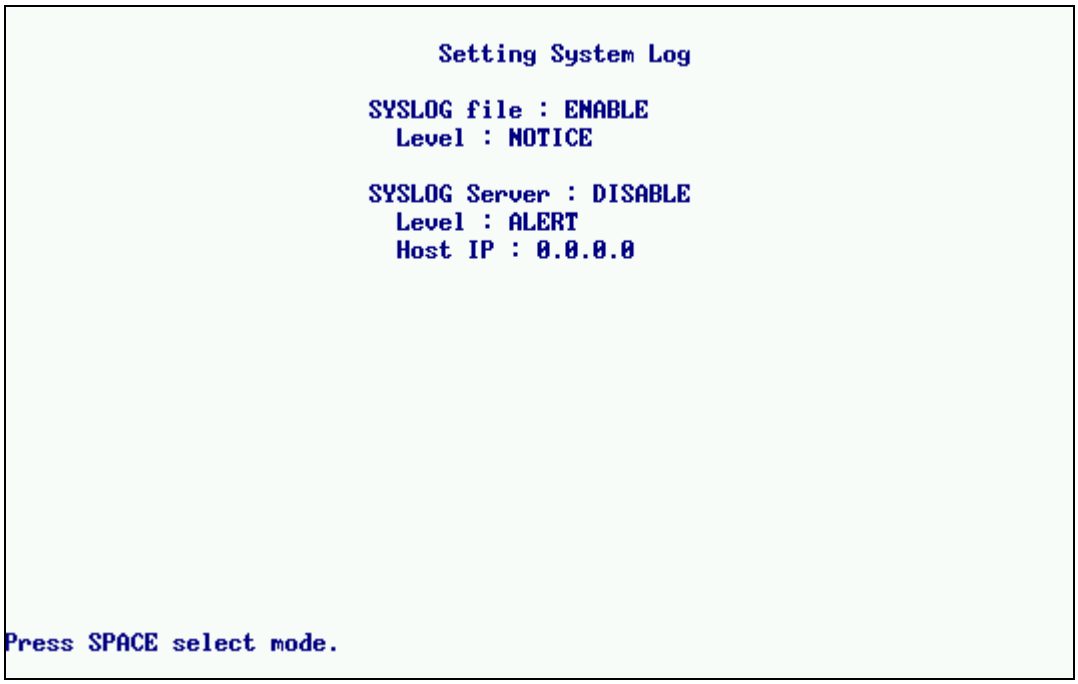
42. Connecting Client List



MAC addresses of all clients associate with AP wireless interface on 3300AG are shown here.

43. System Log





Aphelion 3300AG provides seven system log levels (Level1=DEBUG Level2=EMERGENCY Level3=ALERT Level4=CRITICAL Level5=ERROR Level8=WARNING Level7=NOTICE Level8=INFO) to indicate the level of attention needed for each log. Through setting Syslog server IP address, all system log will send back to the specific log server for centralizing monitoring all Aphelion devices in the network.

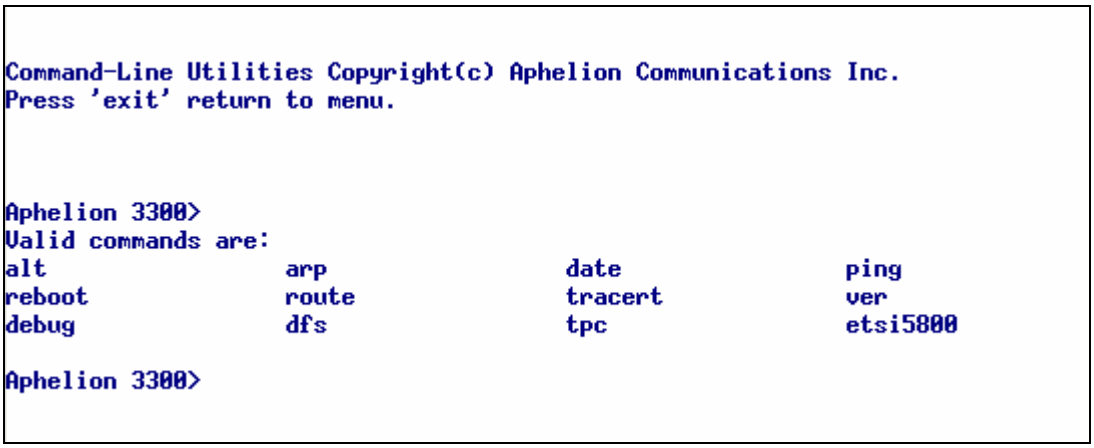
```
                              View System Log


[34]Mar 23 14:19:44 MajorTaskProc: Ctrl MSG Queue<655373>!
[35]Mar 23 14:19:44 exiting on signal 15
[36]Jan  1 00:00:08 syslogd 1.4.1: restart.
[37]Jan  1 00:00:09 SurfConfigLoad: Waiting for global MsgQ..
[38]Jan  1 00:00:11 last message repeated 2 times
[39]Mar 24 07:02:53 MajorTaskProc: Major Task Proc(131072)Ready ...
[40]Mar 24 07:02:53 MajorTaskProc: Ctrl MSG Queue<655373>!
[41]Mar 24 07:02:53 exiting on signal 15
[42]Jan  1 00:00:08 syslogd 1.4.1: restart.
[43]Jan  1 00:00:09 SurfConfigLoad: Waiting for global MsgQ..
[44]Jan  1 00:00:11 last message repeated 2 times
[45]Mar 24 07:08:43 MajorTaskProc: Major Task Proc(131072)Ready ...
[46]Mar 24 07:08:43 MajorTaskProc: Ctrl MSG Queue<655373>!
[47]Mar 24 07:08:43 exiting on signal 15
[48]Mar 24 07:37:32 dhcpd: receive_packet failed on ath0: Network is down



Press 'P', 'N' Previous / Next Page, Press 'C' Clear Log, Press ESC exit menu.
```

44. System Information

```
                              System Information

System Operation Mode : Route
  System Name : Aphelion 3300          Default Gateway : 0.0.0.0
  WLan Country Domain : ETSI           Firmware Version : 0.984

  Ethernet MAC Address : 00:12:9e:80:00:78
         DHCP Server : DISABLE         IP Address : 192.168.1.1/24

  Wireless - 1   MAC Address : 00:12:9e:80:00:79    DHCP Server : ENABLE
         Operation Mode : Wireless Station  ESSID : APHELION0
         Wireless Mode : 802.11bg           Channel : 0 - AUTO
         Encryption Type : NONE             IP Address : 192.168.100.254/24
  Wireless - 2   MAC Address : 00:12:9e:80:00:7a    DHCP Server : ENABLE
         Operation Mode : Access Point      ESSID : APHELION1
         Wireless Mode : 802.11a            Channel : 36 - 5180MHz
         Encryption Type : NONE             IP Address : 10.10.1.254/24
  Wireless - 3   MAC Address : 00:12:9e:80:00:7b    DHCP Server : ENABLE
         Operation Mode : Access Point      ESSID : APHELION2
         Wireless Mode : 802.11bg           Channel : 6 - 2437MHz
         Encryption Type : NONE             IP Address : 10.1.1.254/24
```

System Information summarizes all the configuration and hardware information of the 3300AG.

45. Command Line



- alt
  Alignment tool. alt wireless AC displays the real-time Link Quality, RSSI (receive signal strength indication) and Noise Level continuously. alt is similar to the information in SMT-41, and only available when the wireless is configured as AC.

- arp
  Display ARP information of the 3300AG.

- date
  Display system time.

- ping
  Ping the remote host IP address from the 3300AG.

- reboot
  Reboot the 3300AG.

- route
  Display the route table of 3300AG.

- tracert
  Trace the remote destination IP address to view the routing path.

- ver
  Display the firmware version and the minimum downgradable version of the current firm ware.

- debug

Enable debug mode (by typing debug 1 in command line) displays real-time syslog in command line.

- dfs
  Dynamic Frequency Selection is to avoid the AP using the same channel as military radars. When dfs is on and detects a radar signal, the AP will automatically occupy the next channel available.

- tpc
  Transmit power control to set auto power control on/off. This enables a particular AP to adjust its transmit power to optimal according to the signal strength of the associated AP.

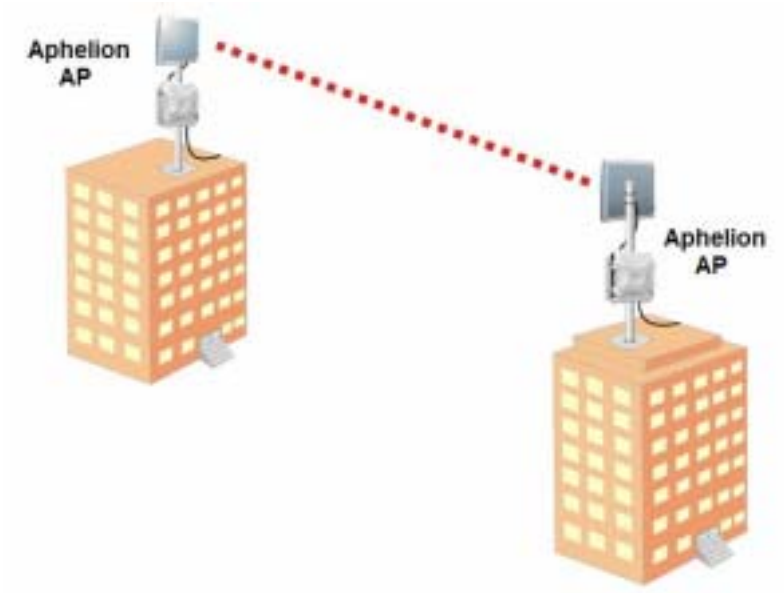
- etsi5000 (only available for 3300 with ETSI standard)
  etsi5000 on releases the 5.7GHz ~ 5.8GHz high frequency bands for 3300AG with ETSI standard.

- exit
  Leave Command Line and back to SMT main page.

Chapter 5. Application Notes

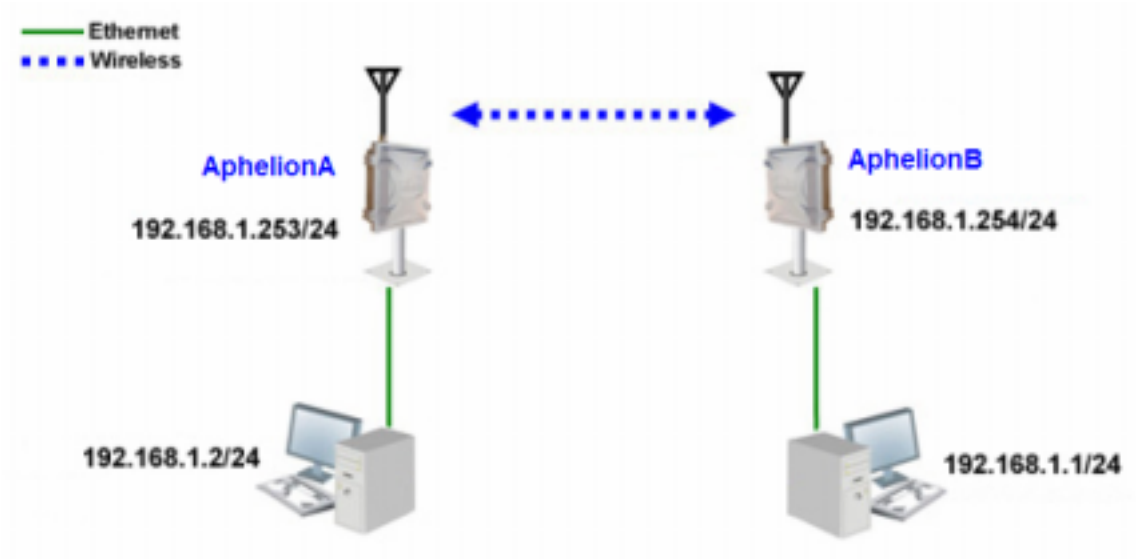
5.1. Point to Point Installation

One of the main applications for Aphelion outdoor AP is to connect two points wirelessly to save the cable cost or overcome certain geographical difficulty to have wire between two points. The figure illustrates a typical point-to-point connection of two buildings a distance apart. Aphelion outdoor APs can act as bridges to connect two points in the same net scope, or act as routers to join two different subnets together. Semi-directional or directional antennas are normally used for this application to have a more focused beam for distant signal transmission. The following sections detail both bridge mode and router mode settings of Aphelion APs for this point to point application.



Bridge Mode

Bridge mode is used when connecting two points in the same net scope. Here, the LAN of 192.168.1.0/24 is used as example to demonstrate how to configure two Aphelion APs for point to point connection in bridge mode. The figure is the topology for this point to point connection with appropriate IP addresses for APs and PCs.



Configurations	AphelionA	AphelionB
System Operation Mode	Bridge	Bridge
Wireless Trunk	Disable	Disable
IP Address	192.168.1.253/24	192.168.1.254/24
Wireless 1	Enable	Enable
ESSID	PTPBridge	PTPBridge
Operation mode	Access Point	Wireless Station
Band	802.11b/g	802.11b/g
Channel	6 2437MHz	AUTO
MAX RF Distance	100	100
Wireless 2	Disable	Disable

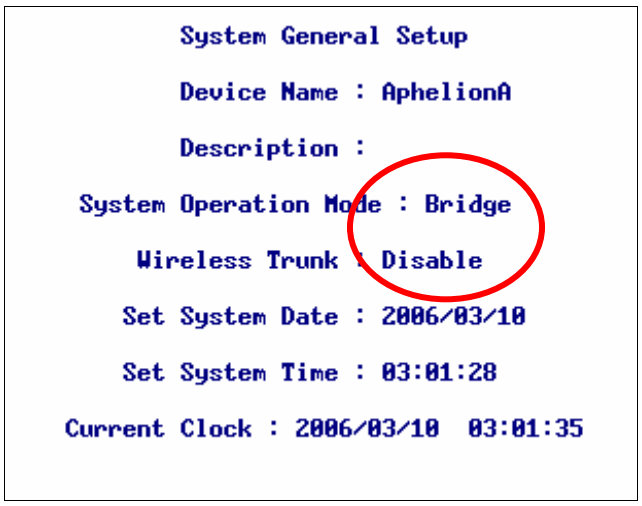
Note :

- This is an example for point to point configuration. Depends on your system, you may use different IP addresses, ESSID, operation frequency and swap AP/AC. It is recommended to set MAX RF Distance when the distance between the two Aphelion 600AGs is greater than 7km.
- Make sure Wireless Trunk is disabled, and Wireless 2 interface is either disable or connect to other devices. If Wireless 2 connects these AphelionA and AphelionB, then the wireless interfaces will create a loop and result in malfunction of the APs.

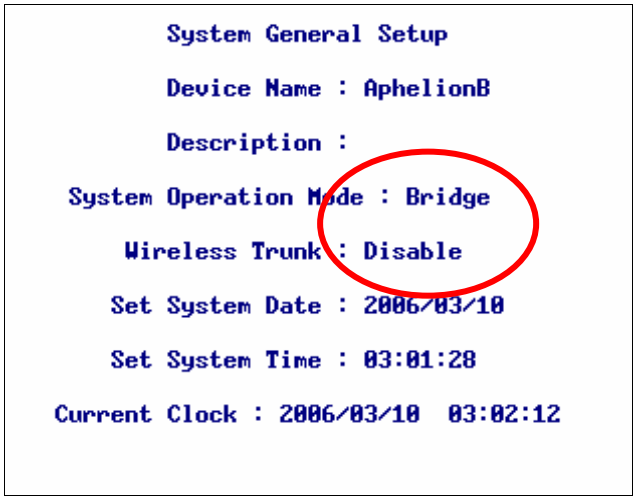
SMT Configuration Step by Step

SMT-11 System General Setup

AphelionA

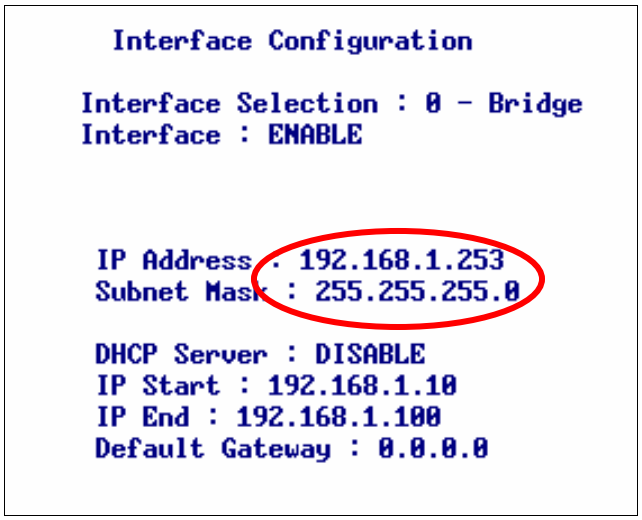

System General Setup
Device Name : AphelionA
Description :
System Operation Mode : Bridge
Wireless Trunk : Disable
Set System Date : 2006/03/10
Set System Time : 03:01:28
Current Clock : 2006/03/10 03:01:35

AphelionB

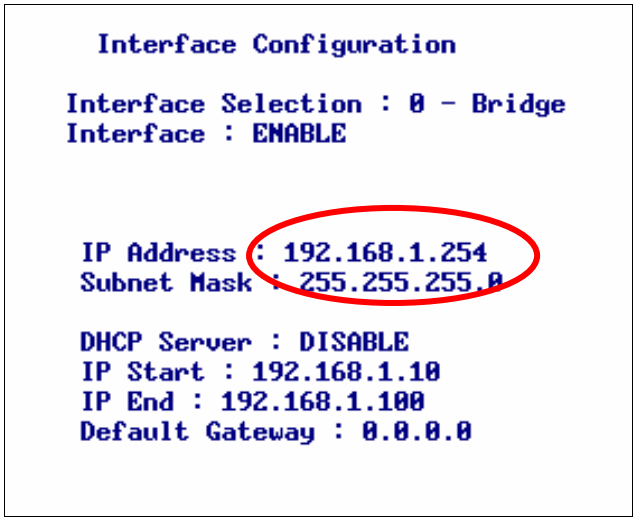

System General Setup
Device Name : AphelionB
Description :
System Operation Mode : Bridge
Wireless Trunk : Disable
Set System Date : 2006/03/10
Set System Time : 03:01:28
Current Clock : 2006/03/10 03:02:12

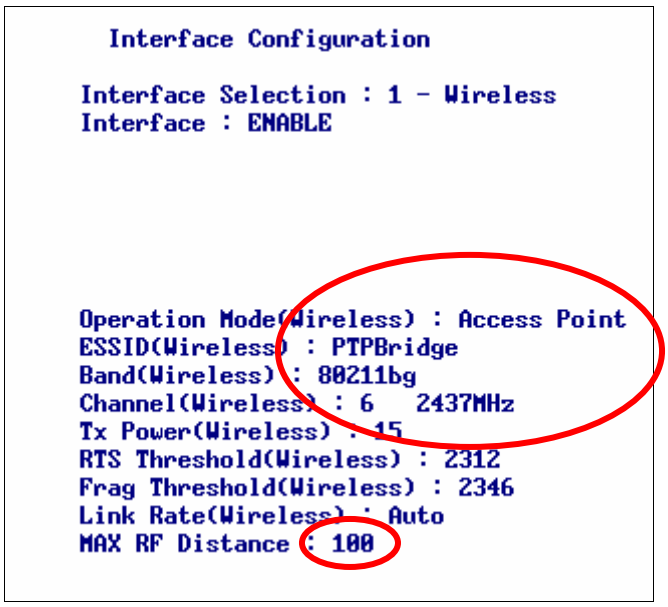
SMT-12 Interface Configuration

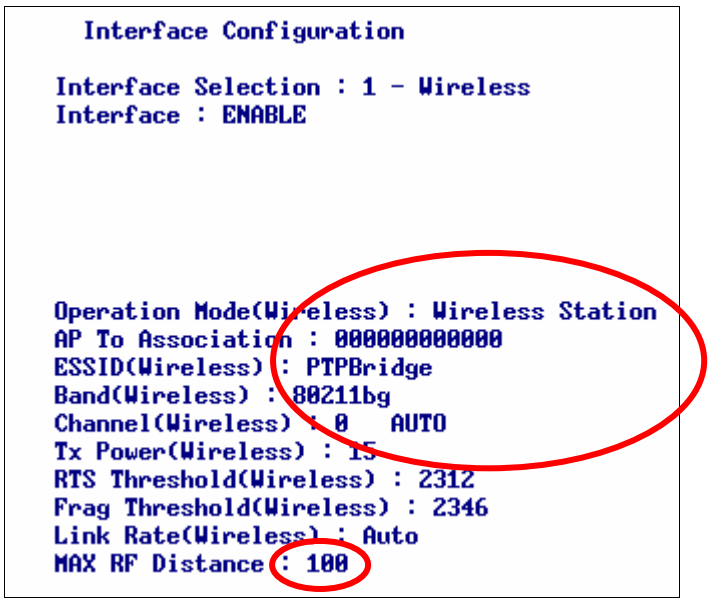
AphelionA



AphelionB



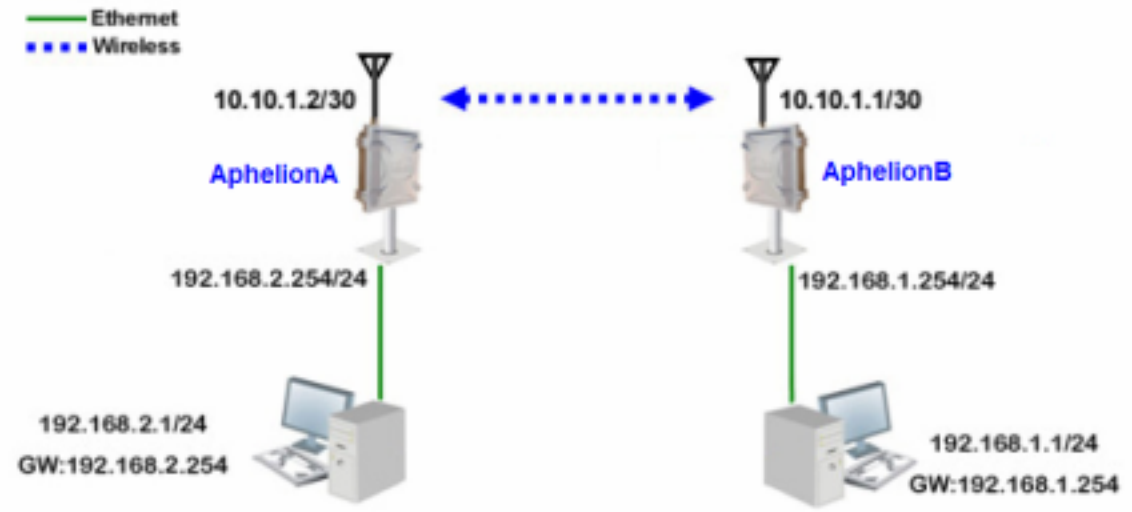



Interface Configuration
Interface Selection : 1 - Wireless
Interface : ENABLE
Operation Mode(Wireless) : Wireless Station
AP To Association : 000000000000
ESSID(Wireless) : PTPBridge
Band(Wireless) : 80211bg
Channel(Wireless) : 0 AUTO
Tx Power(Wireless) : 15
RTS Threshold(Wireless) : 2312
Frag Threshold(Wireless) : 2346
Link Rate(Wireless) : Auto
MAX RF Distance : 100

It is recommended to confirm all the configurations are correct and properly saved by using SMT-44 System Information. If directional antennas are used for this point to point application, please check if the antennas are aligned properly by using SMT-41 Interface Link Status or the command alt in SMT-45 Command Line.

Router Mode

When using point to point to connect two LANs together, router mode configuration is required. The setting of router mode point to point is similar to that of bridge mode, but need to be careful with the setting of IP addresses and gateway to let the data packet be able to go the desired way.



Configurations	AphelionA	AphelionB
System Operation Mode	Route	Route
Wireless Trunk	Disable	Disable
Ethernet IP Address	192.168.2.254/24	192.168.1.254/24
Wireless 1	Enable	Enable
Routing Information	BOTH	BOTH
Wireless 1 IP Address	10.10.1.2/30	10.10.1.1/30
ESSID	PTPRoute	PTPRoute
Operation mode	Access Point	Wireless Station
Band	802.11b/g	802.11b/g
Channel	1 2412MHz	AUTO
MAX RF Distance	100	100
Wireless 2	Disable	Disable
WAN Interface	Wireless 1	Wireless 1
Default Gateway	10.10.1.1	10.10.1.2

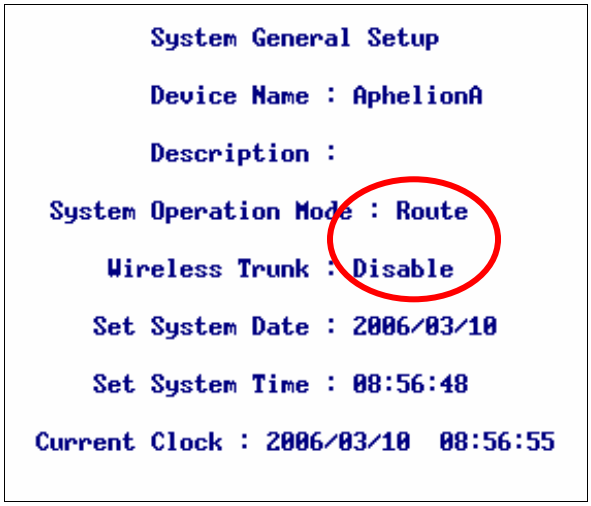
Note :

- This is an example for point to point configuration. Depends on your system, you may use different IP addresses, ESSID, operation frequency and swap AP/AC. It is recommended to set MAX RF Distance when the distance between the two Aphelion 600AGs is greater than 7km.
- Aphelion 600AG is set as a router, so each interface (Ethernet and wireless) needs to have its own IP addresses.
- Routing Information is set to BOTH so 600AG will both receive and give routing information. If Routing Information is set to DISABLE, SMT-14 Routing Configuration needed to be set for AP to know where to set the data packets.
- Aphelion 600AGs are operating in router mode so it is necessary to set WAN interface with appropriate gateway. In this example, because the data packet is only going from one PC to another, 600AGs set each other as default gateway.

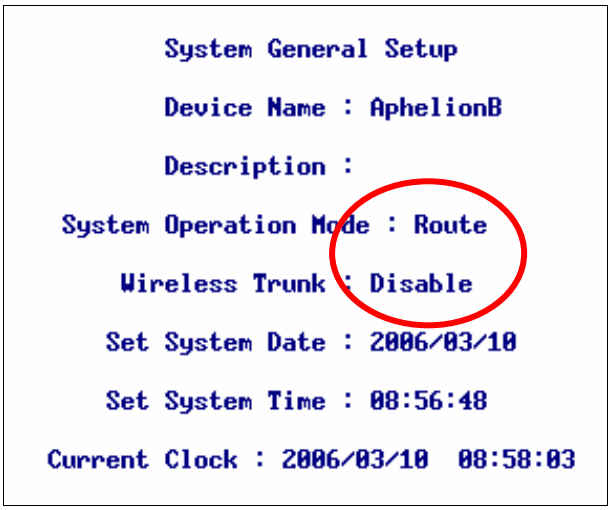
SMT Configuration Step by Step

SMT-11 System General Setup

AphelionA

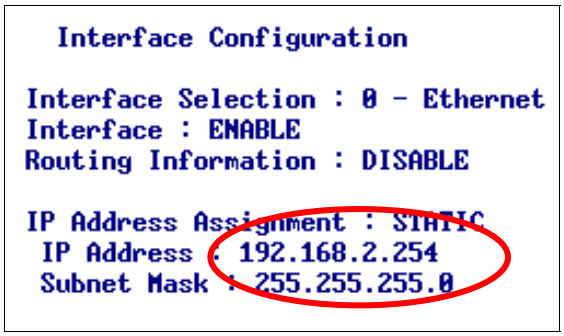

System General Setup
Device Name : AphelionA
Description :
System Operation Mode : Route
Wireless Trunk : Disable
Set System Date : 2006/03/10
Set System Time : 08:56:48
Current Clock : 2006/03/10 08:56:55

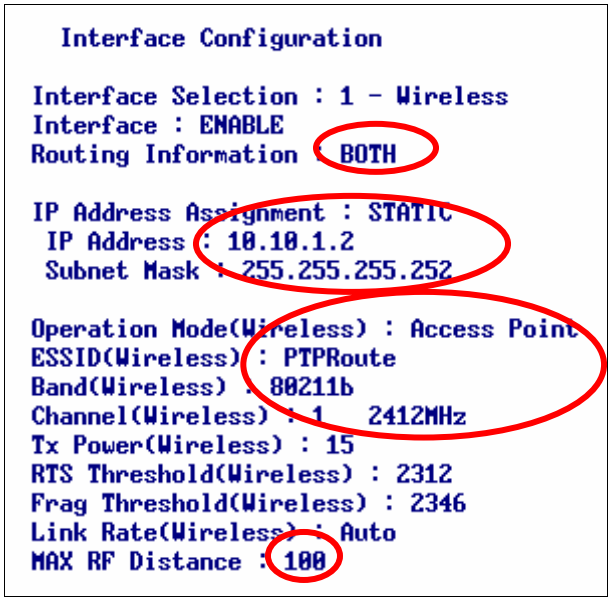
AphelionB


System General Setup
Device Name : AphelionB
Description :
System Operation Mode : Route
Wireless Trunk : Disable
Set System Date : 2006/03/10
Set System Time : 08:56:48
Current Clock : 2006/03/10 08:58:03

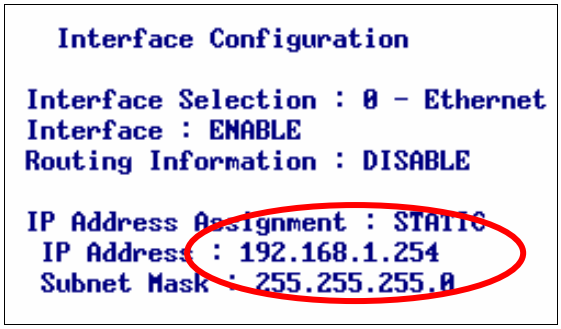
SMT-12 Interface Configuration

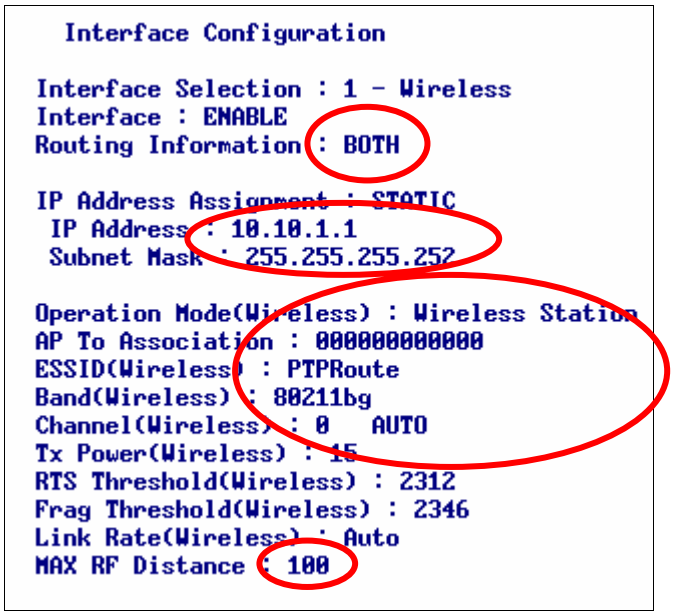
AphelionA


Interface Configuration
Interface Selection : 0 - Ethernet
Interface : ENABLE
Routing Information : DISABLE
IP Address Assignment : STATIC
IP Address : 192.168.2.254
Subnet Mask : 255.255.255.0


Interface Configuration
Interface Selection : 1 - Wireless
Interface : ENABLE
Routing Information : BOTH
IP Address Assignment : STATIC
IP Address : 10.10.1.2
Subnet Mask : 255.255.255.252
Operation Mode(Wireless) : Access Point
ESSID(Wireless) : PTPRoute
Band(Wireless) : 80211b
Channel(Wireless) : 1 2412MHz
Tx Power(Wireless) : 15
RTS Threshold(Wireless) : 2312
Frag Threshold(Wireless) : 2346
Link Rate(Wireless) : Auto
MAX RF Distance : 100

AphelionB


Interface Configuration
Interface Selection : 0 - Ethernet
Interface : ENABLE
Routing Information : DISABLE
IP Address Assignment : STATIC
IP Address : 192.168.1.254
Subnet Mask : 255.255.255.0


Interface Configuration
Interface Selection : 1 - Wireless
Interface : ENABLE
Routing Information : BOTH
IP Address Assignment : STATIC
IP Address : 10.10.1.1
Subnet Mask : 255.255.255.252
Operation Mode(Wireless) : Wireless Station
AP To Association : 000000000000
ESSID(Wireless) : PTPRoute
Band(Wireless) : 80211bg
Channel(Wireless) : 0 AUTO
Tx Power(Wireless) : 15
RTS Threshold(Wireless) : 2312
Frag Threshold(Wireless) : 2346
Link Rate(Wireless) : Auto
MAX RF Distance : 100

SMT-13 Interface Configuration

AphelionA

```
     Assign WAN Interface

WAN Interface selection : 1 - Wireless

IP Address Assignment : STATIC
 IP Address : 10.10.1.2
 Subnetmask : 255.255.255.252

Default Gateway : 10.10.1.1
```

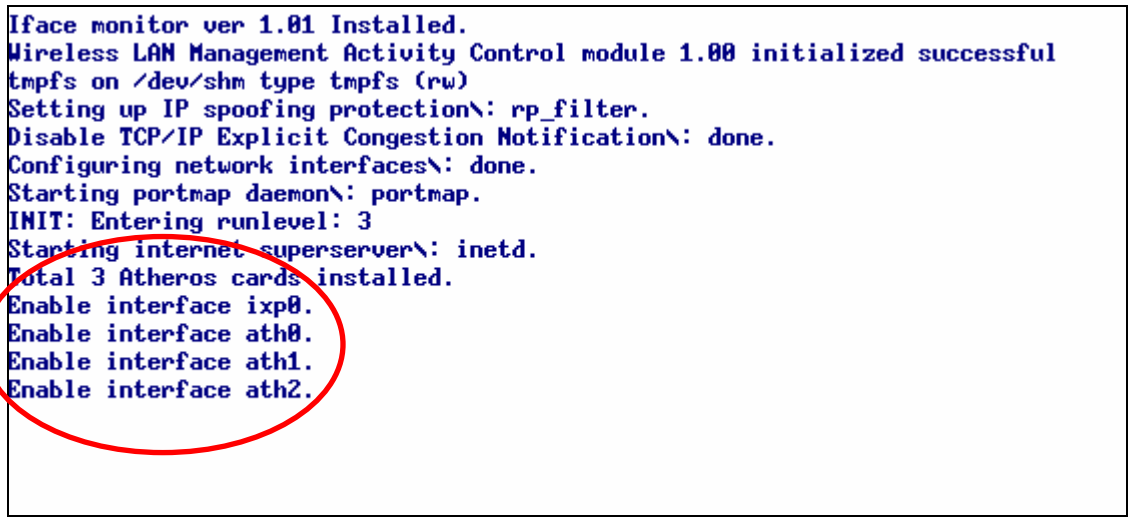
AphelionB

```
     Assign WAN Interface

WAN Interface selection : 1 - Wireless

IP Address Assignment : STATIC
 IP Address : 10.10.1.1
 Subnetmask : 255.255.255.252

Default Gateway : 10.10.10.2
```

It is recommended to confirm all the configurations are correct and properly saved by using SMT-44 System Information. If directional antennas are used for this point to point application, please check if the antennas are aligned properly by using SMT-41 Interface Link Status or the command alt in SMT-45 Command Line.

5.2. Hard Reset to Factory Default

In the case of forgotten system password or any other situations that require setting Aphelion AP back to factory default without entering SMT, there is a reset button on the PCB inside the waterproof housing for hard reset (the picture shows 600AG, the reset button of 3300AG is at the same place on PCB).


Iface monitor ver 1.01 Installed.
Wireless LAN Management Activity Control module 1.00 initialized successful
tmpfs on /dev/shm type tmpfs (rw)
Setting up IP spoofing protection\: rp_filter.
Disable TCP/IP Explicit Congestion Notification\: done.
Configuring network interfaces\: done.
Starting portmap daemon\: portmap.
INIT: Entering runlevel: 3
Starting internet superserver\: inetd.
Total 3 Atheros cards installed.
Enable interface ixp0.
Enable interface ath0.
Enable interface ath1.
Enable interface ath2.

The reset button can be pressed any time after 3300AG has enabled all the interfaces and shows “Enable interface ath2” on the boot log when accessing 3300AG with console.

5.3. Firmware Upgrade

As Aphelion always strives to achieve total customer satisfaction, new features and functions are designed from time to time. To have these new functions in your Aphelion 600AG, you will need to upgrade the firmware.

Please note before performing firmware upgrade:

- Certain versions of firmware are non-interoperable with other versions. Please confirm the interoperability of the new firmware with the existing one in your system.
- If Aphelion APs are upgraded through a daisy chain, please ensure the AP furthest away is upgraded first. As not all the newer version firmware is interoperable with the older one. Also if you upgrade a very old version firmware to a very new one, the configuration of the AP might be set to factory default and make the AP no longer in the same net scope as the existing daisy chain.
- Not all the new version firmware can be downgraded to the previous one. The minimum downgradable version is shown by typing “ver” in SMT-45 Command Line.

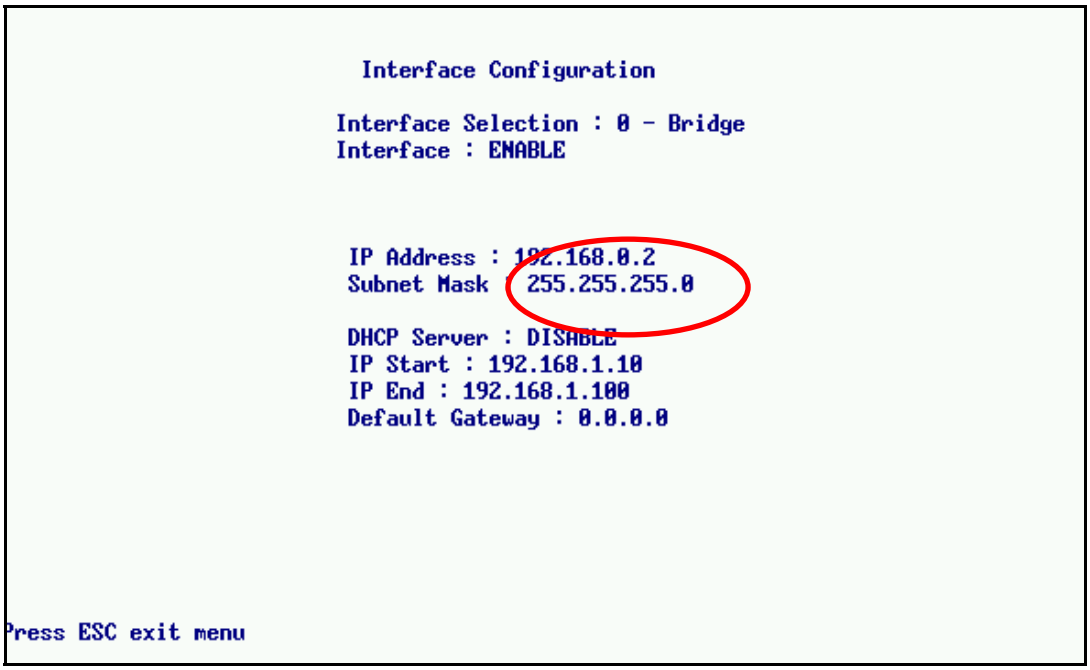
```
Command-Line Utilities Copyright(c) Aphelion Communications Inc.
Press 'exit' return to menu.


Aphelion 3300>ver
Aphelion Communications Software ID is 3300
Version is 0.983 ,min version is 0.982
Kernel size 784200 (0x000bf748)bytes, checksum aa0ae251
Ramdisk size 5549392 (0x0054ad50)bytes, checksum 7bbf1edf
Aphelion Communications Backup Software ID is 3300
Version is 0.983 ,min version is 0.982
Kernel size 784200 (0x000bf748)bytes, checksum aa0ae251
Ramdisk size 5549392 (0x0054ad50)bytes, checksum 7bbf1edf

Aphelion 3300>
```

The easiest way to upgrade Aphelion 3300AG is through the use of SMT and Trivial File Transfer Protocol (TFTP). A PC is made as the TFTP server, and connected to Aphelion AP via the DATA IN port on the PoE unit.

The first step is to configure both the TFTP server (the PC) and the AP to the same net scope, namely the IP address and subnet mask. Here 192.168.0.1/24 for the PC and 192.168.0.2/24 for the AP are used as an example to demonstrate the upgrade procedure with TFTP.

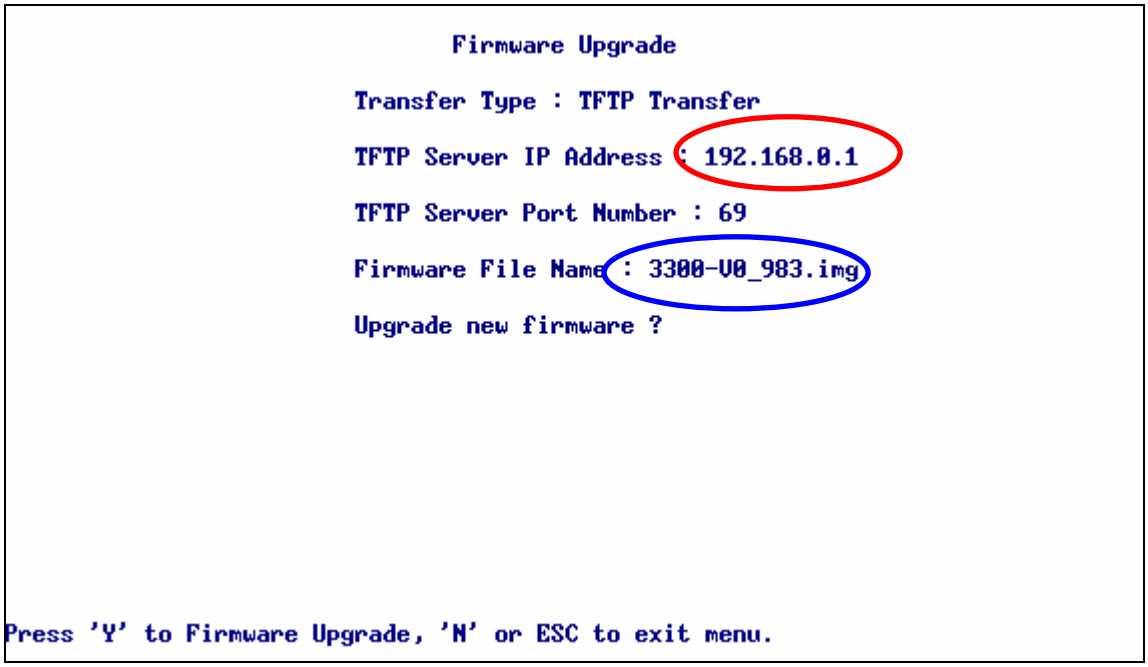
The IP address and subnet mask of PC can be either configured through Internet Protocol (TCP/IP) selection in Network Neighborhood or your usual way. The AP is configured to 192.168.0.2 with subnet mask of 255.255.255.0 in SMT-12, as shown below:

```
                Aphelion Communications Inc.
                   Aphelion 3300 Main Menu

General Configuration                System Management
  11.System General Setup              31.Configuration Management
  12.Interface Configuration           32.Security File Management
  13.Assign WAN Interface              33.Firmware Upgrade
  14.Routing Configuration             34.System reboot

Advanced setting                     System Monitoring
  21.System Password                   41.Interface Link Status
  22.Bandwidth Control                 42.Connecting Client List
  23.DHCP Configuration                43.System log
  24.NAT Configuration                 44.System Information
  25.SNMP Configuration                45.Command Line
  26.Wireless Security Setting         99.Logout

                Enter Menu Selection Number : 12
```



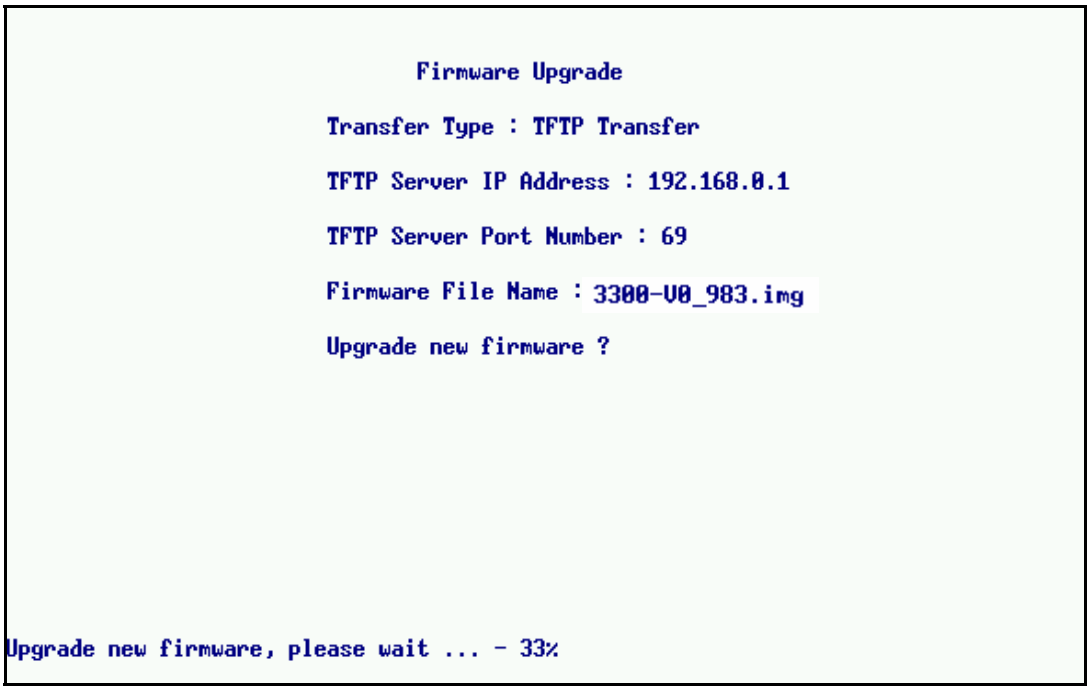
Use the space bar to move the cursor. Press ESC and save the change before exit SMT-12.

Make sure the firmware image file, for example 3300-V0_983.img, is in your TFTP upload/download directory. Then go to SMT-33 Firmware Upgrade.

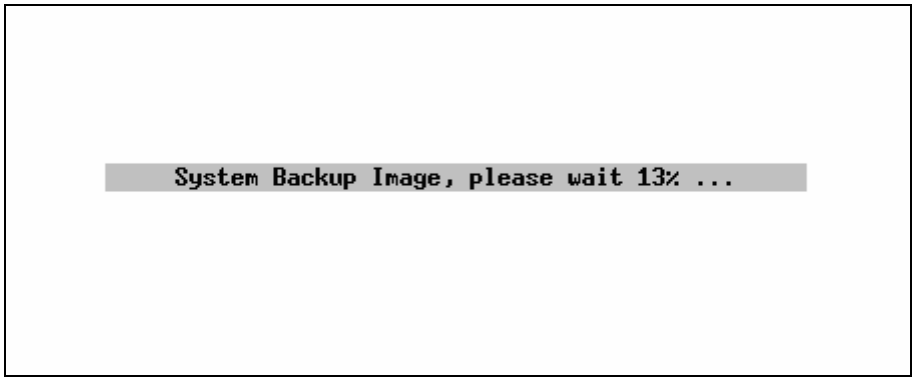

Firmware Upgrade
Transfer Type : TFTP Transfer
TFTP Server IP Address : 192.168.0.1
TFTP Server Port Number : 69
Firmware File Name : 3300-V0_983.img
Upgrade new firmware ?
Press 'Y' to Firmware Upgrade, 'N' or ESC to exit menu.

Enter the IP address of the TFTP server, 192.168.0.1 and the firmware image file 600-v0_982.img in the fields indicated in the circles. Do use the exact file name because it is case sensitive. Move the cursor to the last selection “Upgrade new firmware? “ and press “Y” to begin firmware upgrading. Please keep both the TFTP connection and the power on during the whole upgrading process to ensure a successful upgrading.

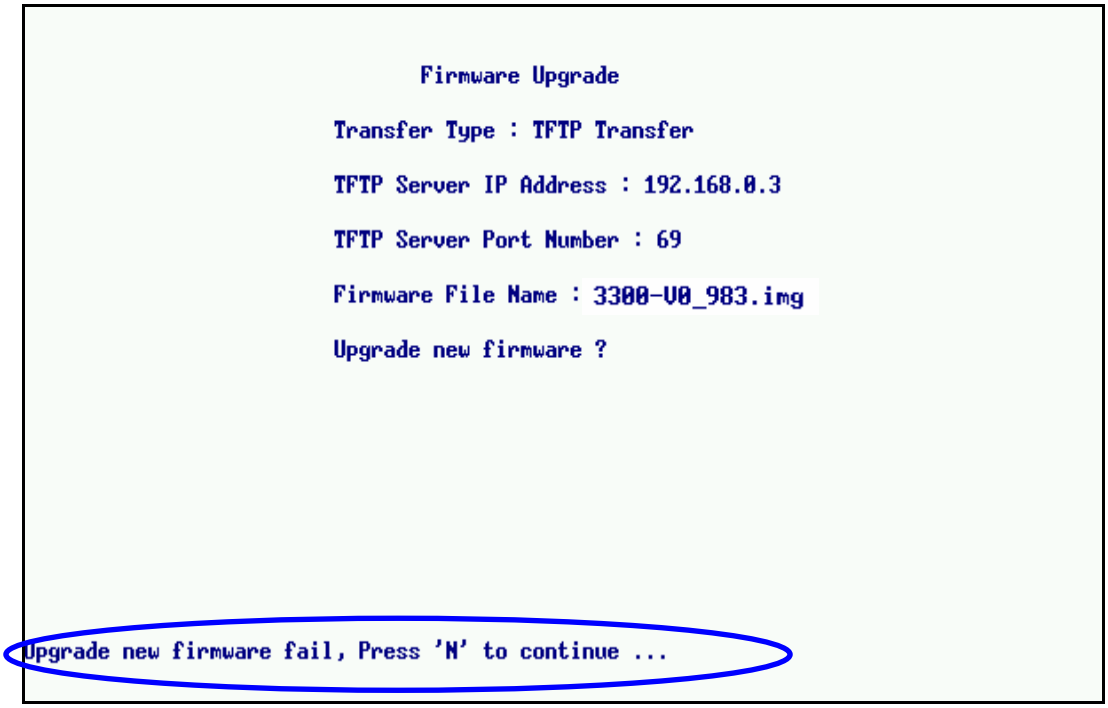
After the firmware has downloaded to the AP successfully, a message will show at the bottom of the screen indicating the percentage of the upgrading.


Firmware Upgrade
Transfer Type : TFTP Transfer
TFTP Server IP Address : 192.168.0.1
TFTP Server Port Number : 69
Firmware File Name : 3300-V0_983.img
Upgrade new firmware ?
Upgrade new firmware, please wait ... - 33%

Please follow the instruction to reboot the AP to make the new firmware take place. After the first successful reboot, the new image will be written to the system backup. Please be patient and keep the power on all the time until the SMT main menu appear on the screen.



If the upgrade is unsuccessful, the following upgrade new firmware fail message will appear.


Firmware Upgrade
Transfer Type : TFTP Transfer
TFTP Server IP Address : 192.168.0.3
TFTP Server Port Number : 69
Firmware File Name : 3300-V0_983.img
Upgrade new firmware ?
Upgrade new firmware fail, Press 'N' to continue ...

Please press “N” to make the cursor active again. Double check if the TFTP server is up and set in the same net scope with the AP. Also check if the firmware image file is in the appropriate directory and all the fields in SMT-33 are entered correctly.

Alternatively, firmware can be upgraded with FTP. The steps of upgrading is similar to that of TFTP upgrade

Appendix

I. Antenna concepts and Installations

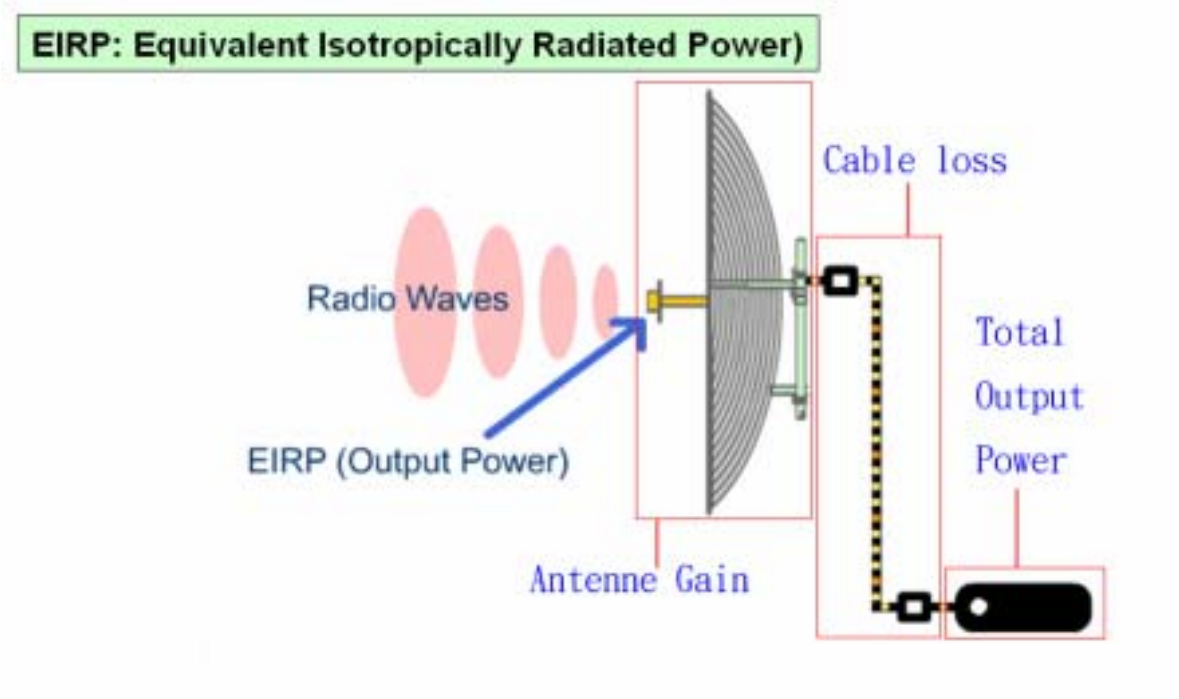
I.1. Basic Terminology

- Transmit Power
  The RF power coming out of the antenna port of a transmitter. It excludes the signal loss of the coaxial cable or the gain of the antenna, and is measured in dBm, Watts or milli-Watts

- Receiver Sensitivity
  The weakest RF signal level (usually in negative dBm) that a radio needs to receive in order to demodulate and decode a data packet without errors.

- Antenna Gain
  The ratio of how much an antenna increases the RF signal over a specified low-gain radiator. Antennas achieve gain by focusing RF energy.

- EIRP
  Equivalent Isotropically Radiated Power is the power actually radiated by the antenna element. It takes into account the antenna gain.



EIRP (dBm), performance of transmitting system
= Total Output Power of device − Cable Loss + Antenna Gain

Free Space Loss (FSL)
As a signal spreads out from a radiating source, the energy spreads out over a larger surface area. As this occurs, the strength of that signal gets weaker. FSL specifies how much the signal has weakened over a given distance, and it is measured in dB.

I.2. RF Path Loss and Transmission Distance Calculation

System Gain (dBm) is the is the total gain of radio without antenna/cable
System Gain = Tx power – Rx Sensitivity

FSL = Tx Power + Tx Antenna Gain + Rx Antenna Gain– Rx Sensitivity
= 32.4 + 20log$_{10}$ *f* (MHz) + 20log$_{10}$ *d* (km)
= 36.4 + 20log$_{10}$ *f* (MHz) + 20log$_{10}$ *d* (mile)
= 92.4 + 20log$_{10}$ *f* (GHz) + 20log$_{10}$ *d* (km)
= 96.4 + 20log$_{10}$ *f* (GHz) + 20log$_{10}$ *d* (mile)
(*f* : radio frequency *d* : distance between the transmitter and the receiver)

Fade Margin is an " extra" signal power added to ensure the proper working of a link.
Fade Margin = System Gain + Antenna Gain – FSL – Cable Loss

A zero Fade Margin indicates the ultimate connection between the transmitter and receiver system. A larger Fade Margin indicates a stronger signal for connection, and a negative Fade Margin indicates connection fail.

Here is an example of Aphelion 600G with 12 dBi antenna (neglect the cable loss in this case).

From the specification of Aphelion 3300AG :
Transmission power : 14 dBm
Receiver sensitivity : -74 dBm
Antenna gain : 12 dBi
Frequency of 802.11b/g : 2.4GHz
According to the specification, we can calculate the Free Space Loss :
FSL = 14 + (12 +12) – (-74) = 112

The ultimate distance between transmit and receive antennas can also be estimated:
FSL = 112 = 32.4 + 20log$_{10}$(2400) + 20log$_{10}$ *d*(km)

d = 3.08 km

II. Wireless Security Concept

II.1. Security for 802.11 Network

Security for 802.11 networks can be simplified into two main components: authentication and encryption. WEP (Wired Equivalent Privacy) is part of the system security of 802.11, and its goals are to provide confidentiality and data integrity, and to protect access to the network infrastructure by rejecting all non-WEP packets.

With 802.11 WEP, all APs and client radio NICs (Network Interface Card) on a particular wireless LAN have to use the same encryption key. A sending station encrypt each frame with a WEP key before transmission, and the receiving station decrypts it using the same key upon reception. This process reduces the risk of eavesdropping and gaining access to the information that carried by the frames.

II.2. Why 802.1x

The major problem with 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool, such as AirSnort or WEPcrack, can monitor your network and decode the encrypted messages. In order to use different keys, you need to manually configure each AP and radio NIC with new common keys. But to renew keys on large networks can be an exhausted task.

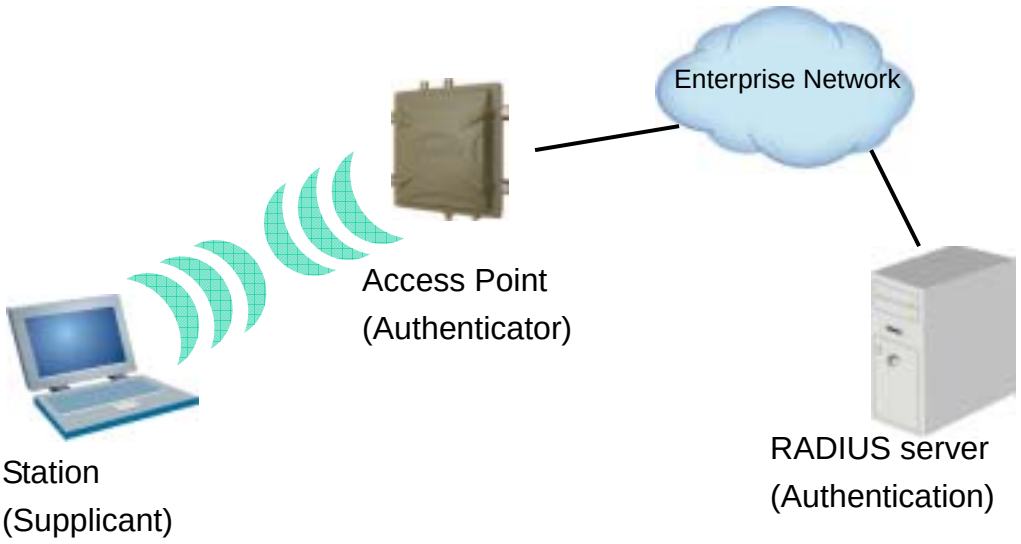
IEEE 802.1x standard helps authenticate and secure wireless LANs. The use of IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. IEEE 802.1x ties EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When utilizing 802.1x, an EAP type needs to be chosen, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), which defines how the authentication takes place.

The software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices. The AP acts as a "pass through" for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant AP. As a result, you can update the EAP authentication type as newer types become available for security change.

II.3. EAP

802.1x uses EAP to relay port access requests between LAN stations ("supplicants"), Ethernet switches or wireless access points ("authenticators"), and RADIUS servers ("authentication servers"). EAP can support multiple authentication mechanisms without having to pre-negotiate a particular one.



Different types of EAP have been defined to support authentication methods and associated network security policies. Here are few widely-deployed EAP types:

- EAP-MD5

  EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP) is a required EAP type that uses the same challenge handshake protocol as PPP-based CHAP, but the challenges and responses are sent as EAP messages. EAP-MD5 CHAP is described in RFC 2284.

A typical use for EAP-MD5 CHAP is to authenticate the credentials of remote access clients by using user name and password security systems. You can also use EAP-MD5 CHAP to test EAP interoperability.

- LEAP (Cisco Lightweight EAP)
  Cisco LEAP is a mutual authentication algorithm that supports dynamic derivation of session keys. With Cisco LEAP, mutual authentication relies on a shared secret, the user login password, which is known by the client and the network, and is used to respond to challenges between the user and the RADIUS server (Remote Authentication Dial-In User Service). As with most password-based authentication algorithms, Cisco LEAP is vulnerable to dictionary attacks.

- EAP-TLS (EAP with Transport Layer Security)
  TLS provides mutual authentication, integrity-protected negotiation, and key exchange between two endpoints. Therefore, EAP-TLS that includes support for fragmentation and reassembly provides for these TLS mechanisms within EAP. Windows CE .NET supports EAP-TLS.

- EAP-TTLS (EAP with Tunneled TLS)
  In EAP-TTLS, only a RADIUS Server needs to acquire a Digital Certificate, but a wireless station needs to import the CA (Certificate Authority) so that it can verify the received certificate. The RADIUS server sends its certificate for station verification. A secure tunnel will be created at this stage. The station then sends its username, password via the secure tunnel. After authentication, both ends begin dynamic key exchanging as in EAP-TLS.

- PEAP (Protected EAP)
  PEAP is an EAP extension for Windows CE .NET that enhances the security of the authentication phase. PEAP provides the security framework for mutual authentication between an EAP client and an EAP server. PEAP is not as secure as TLS, but it has the advantage of being able to use username/password authentication instead of client certificate authentication.

II.4. RADIUS Overview

RADIUS (Remote Authentication Dial-In User Service) is an Internet draft standard protocol. RADIUS is always connected with all kinds of NAS (Network Access Server), such as router, switch, RAS, and all kinds of NAS possible to take responsibility for authentication, authorization, and accounting in telecommunication networks.

In large networks, security information can be scattered throughout the network on different devices. RADIUS allows user information to be stored on one host, minimizing the risk of security loopholes. All authentication and access to network services is managed by the host functioning as the RADIUS server.

The RADIUS messages which are sent between RADIUS server and RADIUS client are defined by RFCs 2865 and 2866 as following types:

- Access-request
  A message sent from an AC to an access server in order to request authentication and authorization for a network access connection attempt.

- Access-accept
  A message sent from an access server to an AC to response the access-request message which informs the RADIUS client that the connection attempt is authenticated and authorized.

- Access-reject
  A message sent from an access server to an AC to response the access-request message which informs the RADIUS client that the connection attempt is not authenticated or authorized.

- Access-challenge
  A message sent by a RADIUS client to specify accounting information for a connection that was accepted.

- Accounting-Request
  A message sent by a RADIUS client to specify accounting information for a connection that was accepted.

- Accounting-Response
  A message sent by access server to acknowledge the successful receipt and processing of the Accounting-Request message

RADIUS messages are sent as User Datagram Protocol (UDP) messages. UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages.

III. Glossary

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - An “Access Point Mode” and “Wireless Station Mode” connection topology creating a wireless backbone trunk to reach multi-hopping between each wireless node.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

Download - To receive a file transmitted over a network.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node - A network junction or connection point, typically a computer or work station.

Packet - A unit of data sent over a network.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

Upgrade - To replace existing software or firmware with a newer version.

WEP (**W**ired **E**quivalent **P**rivacy) - An optional cryptographic confidentiality algorithm specified
by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.